CENTRO UNIVERSITÁRIO EUROAMERICANO – UNIEURO
PRÓ-REITORIA E PÓS-GRADUAÇÃO, PESQUISA E EXTENSÃO
COORDENAÇÃO DE PÓS-GRADUAÇÃO LATO SENSU
MBA EM GOVERNANÇA DE TI

LEONARDO RAMOS PAZ
TÂNIA DA SILVA MOUTINHO
VITOR DUTRA FREIRE

Governança de TI na Administração Pública Federal: Avanços e Desafios

BRASÍLIA
2013

LEONARDO RAMOS PAZ
TÂNIA DA SILVA MOUTINHO
VITOR DUTRA FREIRE

Governança de TI na Administração Pública Federal: Avanços e Desafios

Trabalho de Conclusão de Curso – Monografia, apresentada como pré-requisito parcial para conclusão do curso de MBA em Governança de TI do Centro Universitário EUROAMERICANO – UNIEURO.

EUROAMERICANO – UNIEURO.
Orientadora: Prof.ª Dra. Edna Dias Canedo

BRASÍLIA
2013

LEONARDO RAMOS PAZ
TÂNIA DA SILVA MOUTINHO
VITOR DUTRA FREIRE

Governança de TI na Administração Pública Federal: Avanços e Desafios

Esta monografia foi julgada adequada à obtenção do grau de Especialista em Governança de TI e aprovada em sua forma final pelo curso de MBA em Governança de TI do Centro Universitário EUROAMERICANO – UNIEURO.

Data de aprovação:

RESUMO

Esta monografia enfoca a aplicação da Governança de Tecnologia da Informação no âmbito da Administração Pública Federal. O estudo se baseia na análise documental dos estudos de caso realizados pelo TCU nos anos de 2007, 2010 e 2012, e nas ações indutoras do Controle Externo realizadas pelo órgão para incentivar a adoção de boas práticas de Governança nos órgãos federais, comparando as boas práticas adotadas com aquelas recomendadas pelos principais modelos de mercado. O objetivo deste trabalho é apresentar o resultado dos três levantamentos de informações realizados pelo TCU, a situação atual da governança de TI na Administração Pública Federal, os avanços realizados desde que o TCU iniciou o seu estudo e os desafios a serem vencidos.

Palavras-Chave: Governança de TI, Tribunal de Contas da União, Administração Pública Federal, Boas Práticas em TI.

ABSTRACT

This monograph focuses on the application of Information Technology Governance within the Brazilian Federal Public Administration. The study is based on documental analysis of case studies carried out by the Court of Audit (TCU) in the years 2007, 2010 and 2012, and on the inducing external control actions performed by the Court to encourage the adoption of governance best practices in federal agencies, comparing the best practices adopted with those recommended by leading market models. The objective of this paper is to present the results of the three surveys conducted by TCU, the current state of IT governance in the Federal Public Administration, the progress made since the TCU began its study and challenges yet to be overcome.

Key-Words: IT Governance, Court of Audit, Federal Public Administration, IT Best Practices.

Sumário

1. Introdução

1.1. Problema e Justificativa

Historicamente, a Administração Pública brasileira, seja ela federal, estadual ou municipal, sempre teve de se preocupar com diversos assuntos essenciais à população, como, por exemplo, saúde, educação e transporte. No passado, esses eram os serviços que mais afetavam a população. Atualmente, ainda continuam a ser essenciais, porém ao lado de um "novo" serviço, que dá suporte a todos os outros: a tecnologia da informação (TI).

Antigamente, a tecnologia era essencialmente vista como operacional e uma fonte de custos para as organizações públicas e privadas. Os investimentos em tecnologia eram ínfimos e o espaço reservado para os profissionais de tecnologia era "insalubre" (ainda existe, na memória de muitos, as imagens dos antigos "Centros de Processamento de Dados - CPDs", que normalmente ficavam numa pequena sala no subsolo das organizações).

Com o passar do tempo, a tecnologia tomou um papel central nas organizações. Deixando o título de "operacional", para ganhar vários outros, como: essencial, viabilizadora, estratégica etc. Os responsáveis pelas atividades-fim das organizações perceberam que a tecnologia da informação é essencial para o negócio, que ela viabiliza a prestação dos serviços e que tem um papel-chave na estratégia de negócio.

O Tribunal de Contas da União (TCU) diz que "é notória a dependência que as organizações atuais têm dos sistemas informatizados. Cresce a quantidade e a complexidade de sistemas computacionais que controlam os mais variados tipos de operações e o próprio fluxo de informações nas organizações. Com efeito, a Administração Pública brasileira, reflexo da própria sociedade, está cada vez mais adotando o computador como ferramenta indissociável na busca da excelência na produção de bens e na prestação de serviços. Grande parte dos órgãos e entidades sob a jurisdição do Tribunal já utiliza maciçamente a tecnologia da informação para automatizar sua operação, registrar, processar, manter e apresentar informações."

Na Administração Pública, juntamente com o ganho de espaço da tecnologia da informação, surgiu a necessidade de maior controle e aplicação de boas práticas em TI.

De acordo com o Tribunal de Contas da União:

> "A informatização crescente reclama especial atenção das organizações, uma vez que a utilização da tecnologia da informação para manipulação e armazenamento de dados introduz novos riscos e aumenta a fragilidade de algumas atividades. Assim, torna-se essencial a atenção dos gestores públicos para as questões relacionadas à segurança da tecnologia da informação e à qualidade dos sistemas informatizados disponíveis ao público".

Dessa forma, com o objetivo de fiscalizar a gestão e o uso de recursos de TI na Administração Pública Federal (APF), o Tribunal de Contas da União criou, em agosto de 2006, a Secretaria de Fiscalização de Tecnologia da Informação - SEFTI.

De acordo com o Tribunal, "essa secretaria especializada, criada em agosto de 2006 para fiscalizar a gestão e o uso de recursos de TI na Administração Pública Federal, conduz trabalhos específicos em fiscalização de Tecnologia da Informação e serve de suporte às demais Secretarias do Tribunal, atuando, sempre que solicitada, em uma estrutura matricial de fiscalização. Além disso, elabora e dissemina metodologias, manuais, notas técnicas e procedimentos para planejamento e execução de fiscalizações de tecnologia da informação, visando maior qualidade dos trabalhos de fiscalização nessa área. A SEFTI também realiza ações sistematizadas de relacionamento, divulgação e troca de conhecimentos com a sociedade, o Congresso Nacional e os Gestores Públicos por meio do Diálogo Público de TI".

Ainda segundo a Corte de Contas, "suas três Divisões de Governança de Tecnologia da Informação possuem a atribuição de coordenação e realização de fiscalizações da governança de TI, nos sistemas informatizados da Administração Pública, nas iniciativas de governo eletrônico e na gestão dos recursos de tecnologia da informação, bem como a missão de coordenação e realização de fiscalizações em editais de licitação, em contratos e em processos de aquisições diretas".

Uma das principais preocupações do TCU é a situação da governança de TI na Administração Pública. Segundo o Tribunal, "um dos grandes desafios da Administração

Pública Federal na atualidade é a elevação do seu grau de governança. O Tribunal de Contas da União, como órgão de controle externo, tem um papel de destaque no aperfeiçoamento dessa área. Nesse contexto, a governança de tecnologia da informação (TI) é essencial para que se atinja esse objetivo. A TI é o verdadeiro motor das organizações modernas podendo tanto impulsioná-las muito adiante como emperrar o seu progresso".

Devido à complexidade e à dimensão estratégica da governança de TI e com o intuito de obter informações acerca do tema na APF, a SEFTI, a partir de 2007, passou a realizar Levantamentos acerca da Governança de Tecnologia da Informação na Administração Pública Federal.

Atualmente, este levantamento de informações possui três edições: 2007, 2010 e 2012. De acordo com a Corte, as informações obtidas no levantamento são utilizadas na elaboração do planejamento das fiscalizações a serem realizadas pelo Tribunal com o intuito de aumentar a eficiência e eficácia de suas ações. Ainda segundo o TCU, "o resultado final esperado é a indução de melhorias na governança de TI na Administração Pública Federal e, consequentemente, sua modernização e aperfeiçoamento".

1.2. Objetivos do Trabalho

1.2.1. Objetivo Geral

O objetivo deste trabalho é apresentar, por meio de análise documental, o resultado dos três levantamentos de informações realizados pelo TCU, a situação atual da governança de TI na Administração Pública Federal, os avanços e os desafios.

1.2.2. Objetivos Específicos

São objetivos específicos deste trabalho:

a) descrever o estudo realizado pelo TCU em relação à Governança de TI na Administração Pública Federal;
b) analisar os resultados de alguns estudos realizados pelo TCU;
c) mostrar os avanços já conseguidos desde que o levantamento foi realizado;
d) mostrar os desafios que ainda devem ser superados na Administração Pública Federal.

Por fim, segundo o IT Governance Institute (2007), "a governança de TI é de responsabilidade da alta administração (incluindo diretores e executivos), na liderança, nas estruturas organizacionais e nos processos que garantem que a TI da empresa sustente e estenda as estratégias e objetivos da organização".

Para viabilizar a governança de TI, institutos e organizações internacionais (e até mesmo brasileiros) desenvolveram *frameworks* de tecnologia da informação, que são, em resumo, conjuntos das melhores práticas de governança de TI sobre determinado tema.

O *IT Governance Institute* - ITGI, estabelecido em 1998 para melhoria do pensamento e dos padrões internacionais de direção e controle da tecnologia da informação nas organizações, editou um dos *frameworks* mais utilizados em governança de TI quando o assunto é controle e auditoria: o CobiT (Control Objectives for Information and related Technology).

De acordo com o ITGI, "o Control Objectives for Information and related Technology (CobiT®) fornece boas práticas através de um modelo de domínios e processos e apresenta atividades em uma estrutura lógica e gerenciável. As boas práticas do CobiT representam o consenso de especialistas. Elas são fortemente focadas mais nos controles e menos na execução. Essas práticas irão ajudar a otimizar os investimentos em TI, assegurar a entrega dos serviços e prover métricas para julgar quando as coisas saem erradas".

Ainda segundo o instituto, "o foco em processos do CobiT é ilustrado por um modelo de processos de TI subdivididos em quatro domínios e 34 processos (CobiT 4.1) em linha com as áreas responsáveis por planejar, construir, executar e monitorar, provendo assim uma visão total da área de TI".

Por sua vez, outra importante estrutura responsável pela governança de TI é o *Cabinet Office*, do Reino Unido, que é responsável pelo framework ITIL (*Information Technology Infrastructure Library*). O ITIL foi desenvolvido no final dos anos 1980 e oferece as melhores práticas na prestação de serviços de tecnologia. O principal objetivo do ITIL é entregar valor para o negócio por meio da prestação de serviços de TI.

O framework é considerado neutro, visto que não se baseia em nenhuma tecnologia em particular e também é tido como não-prescritivo, já que as práticas são testadas pelo tempo e têm aplicabilidade a todos os tipos de organizações de serviço, nos setores público e privado.

Com relação à gerência de projetos, temos o guia PMBOK (Project Management Body of Knowledge), do PMI (Project Management Institute). Segundo o PMI, o objetivo do PMBOK é "identificar o subconjunto do conjunto de conhecimentos em gerenciamento de projetos que é amplamente reconhecido como boa prática".

Por fim, citando um modelo brasileiro, quando o assunto é software, temos o MPS.BR (Melhoria de Processo de Software Brasileiro), criado em dezembro de 2003, coordenado pela Associação para Promoção da Excelência do Software Brasileiro (SOFTEX), que conta com apoio do Ministério da Ciência e Tecnologia (MCT), Financiadora de Estudos e Projetos (FINEP), Serviço Brasileiro de Apoio às Micro e Pequenas Empresas (SEBRAE) e Banco Interamericano de Desenvolvimento (BID).

Segundo a SOFTEX, "com o MPS-SW foi possível estabelecer um caminho economicamente viável para que organizações, incluindo as pequenas e médias empresas, alcancem os benefícios da melhoria de processos e da utilização de boas práticas da engenharia de software em um intervalo de tempo razoável. Ele trouxe para a indústria nacional ganhos comprovados de competitividade, por isso é considerado um marco que representa a evolução da qualidade do software desenvolvido no país".

Na Administração Pública Federal, a governança de TI avança (em alguns órgãos, ainda a passos lentos), devido à atuação do Tribunal de Contas da União (TCU), por meio de sua unidade vinculada, a SEFTI - Secretaria de Fiscalização de Tecnologia da Informação.

De acordo com a Constituição Federal brasileira, em seu art. 71, caput, compete ao Tribunal de Contas da União auxiliar o Congresso Nacional no exercício do controle externo.

No Dicionário Houaiss, a palavra "controle" possui várias acepções, das quais interessam: ato ou efeito de controlar; monitoração, fiscalização ou exame minucioso, que obedece a determinadas expectativas, normas, convenções etc.; e poder, domínio ou autoridade sobre alguém ou algo.

A Escola Clássica de Fayol identificava no controle uma das funções administrativas essenciais no ciclo que compreendia planejar, organizar, dirigir e controlar. Segundo Chiavenato (CHIAVENATO, 2006, p.447), o controle consiste na "função administrativa que

monitora e avalia as atividades e resultados alcançados para assegurar que o planejamento, organização e direção sejam bem sucedidos".

Mais especificamente, o controle externo, atribuição precípua do TCU, segundo Pardini (1997 apud BUGARIN, 2004, p. 40):

> "Em sentido orgânico e técnico, é, em resumo, todo controle exercido por um Poder ou órgão sobre a administração de outros. Nesse sentido, é controle externo, o que o Judiciário efetua sobre os atos dos demais Poderes. É controle externo o que a administração direta realiza sobre as entidades da administração indireta. É controle externo o que o Legislativo exerce sobre a administração direta e indireta dos demais poderes. Na terminologia adotada pela Constituição, apenas este último é que recebe a denominação jurídico-constitucional de controle externo (CF: arts. 31 e 70 a 74), denominação esta repetida especificamente em outros textos infraconstitucionais, como, por exemplo, a Lei n° 8.443/92".

Dessa forma, investido de atribuições constitucionais, por meio do controle externo, o Tribunal de Contas da União exerce a "fiscalização contábil, financeira, orçamentária, operacional e patrimonial da União e das entidades da administração direta e indireta, quanto à legalidade, legitimidade, economicidade, aplicação das subvenções e renúncia de receitas, será exercida pelo Congresso Nacional, mediante controle externo, e pelo sistema de controle interno de cada Poder" (Constituição Federal, art. 70, caput).

Para auxiliar no controle relativo à tecnologia da informação dos órgãos e entidades da Administração Pública Federal, o TCU criou a SEFTI, que, segundo a Resolução/TCU n° 193, de 9 de agosto de 2006, "tem por finalidade fiscalizar a gestão e o uso de recursos de Tecnologia da Informação pela Administração Pública Federal".

De acordo com o Tribunal, o negócio da unidade é o controle externo da governança de tecnologia da informação na Administração Pública Federal; sua missão é assegurar que

a tecnologia da informação agregue valor ao negócio da Administração Pública Federal em benefício da sociedade e sua visão é ser unidade de excelência no controle e no aperfeiçoamento da governança de tecnologia da informação.

É por meio da SEFTI que o TCU vem realizando estudos com o objetivo de conhecer o nível de maturidade da tecnologia da informação da Administração Pública Federal nos mais variados temas, como segurança da informação, contratação de bens e serviços de TI, governança de TI etc.

Com o objetivo de obter essas informações o Tribunal de Contas da União vem realizando levantamentos de informações sobre a governança de TI na Administração Pública Federal.

Por meio da Portaria-SEGECEX n° 15, de 9 de maio de 2011, o TCU disciplina a realização de levantamentos e aprova, em caráter preliminar, o documento *Padrões de Levantamento.*

De acordo com a Corte de Contas, os levantamentos se destinam a conhecer as organizações e o funcionamento dos órgãos/entidades da Administração Pública Federal, identificar objetos e instrumentos de fiscalização e avaliar a viabilidade da realização de fiscalizações.

A portaria mencionada dispõe que o levantamento tem como principais objetivos:

> "2.1. Propiciar que as unidades técnicas obtenham e mantenham conhecimento acerca das unidades jurisdicionadas que compõem a sua clientela. Dessa forma, seus resultados devem servir de subsídio para a criação e a manutenção de pastas permanentes, com informações atualizadas e catalogadas sobre as unidades jurisdicionadas ou outros objetos de fiscalização.
> 2.2. Identificar carências de atuação do TCU em relação a algum tema ou potenciais áreas de fiscalização. Dessa forma, o encaminhamento do trabalho poderá incluir propostas de ações de controle".

Desde que a SEFTI foi criada, em 2006, o Tribunal já realizou três levantamentos de informações de governança de TI. Os levantamentos são datados de 2007, 2010 e 2012. Esses levantamentos e suas implicações na Administração Pública Federal constituem objeto de estudo desse trabalho.

3. Desenvolvimento

3.1. Levantamento de Informações de 2007

O levantamento de Informações de governança de Tecnologia da Informação de 2007, realizado pelo Tribunal de Contas da União, foi autorizado pelo Acórdão 435/2007 - Plenário, com o objetivo de coletar informações acerca dos processos de aquisição de bens e serviços de TI, de segurança da informação, de gestão de recursos humanos de TI e das principais bases de dados e sistemas da Administração Pública Federal.

Com o levantamento o TCU elaborou um mapa com a situação da governança de TI na Administração Pública Federal e, em paralelo, identificou os principais sistemas e bases de dados da Administração Pública Federal.

Durante a fase de planejamento do levantamento, a equipe responsável formulou as seguintes questões de auditoria:

- É feito o planejamento estratégico institucional e de TI nos órgãos/entidades?
- Qual o perfil dos recursos humanos da área de TI quanto à formação, vínculo com a organização e pré-requisitos para ocupação de funções comissionadas?
- São efetuados ações e procedimentos que contribuam para a minimização dos riscos e o aumento no nível de segurança das informações dos órgãos/entidades?
- O desenvolvimento de sistemas segue alguma metodologia? Os órgãos/entidades mantêm inventário dos principais sistemas e bases de dados?
- Os órgãos/entidades gerenciam os acordos de níveis de serviço tanto quanto prestam internamente como quando contratam externamente serviços de TI?
- O processo de contratação de bens e serviços de TI é formalizado, padronizado e judicioso quanto ao custo, à oportunidade e aos benefícios advindos das contratações de TI?
- O processo de gestão dos contratos de TI é formalizado, padronizado e executado?

- Os órgãos/entidades solicitam o orçamento de TI com base no planejamento da área e controlam os gastos com TI ao longo do exercício financeiro?
- Os órgãos/entidades realizam auditorias de TI nas suas organizações?

De acordo com os dados do levantamento, foram selecionados como amostra 333 órgãos/entidades da Administração Pública Federal. Desses órgãos/entidades, 29 responderam em conjunto com outros órgãos/entidades e 14 não se consideraram integrantes da APF, apesar de serem jurisdicionados ao TCU, em especial os que fazem parte do Sistema 'S'. Outros 25 órgãos/entidades não responderam à pesquisa e 10 não completaram a quantidade mínima estabelecida de respostas. Dessa forma, 255 órgãos/entidades participaram efetivamente do levantamento.

Foi elaborado um questionário composto de 39 perguntas baseadas nas normas técnicas brasileiras NBR ISO/IEC 17799:2005, NBR ISO/IEC 15999-1:2007 e no *Control Objectives for Information and related Technology 4.1* (Cobit 4.1).

A norma NBR ISO/IEC 17799:2005, renumerada para NBR ISO/IEC 27002:2005, é um código de boas práticas em segurança da informação. Essa norma fornece recomendações em gestão da segurança da informação e tem como propósito prover uma base comum para o desenvolvimento de normas de segurança organizacional e das práticas efetivas de gestão da segurança, e prover confiança nos relacionamentos entre as organizações.

Por sua vez, a norma NBR 15999-1:2007 é o código de práticas para a gestão de continuidade de negócios, baseada na norma inglesa BSI 25999:2006 e internalizada no Brasil pela ABNT em outubro de 2007. Seu objetivo é fornecer um sistema baseado nas boas práticas de gestão de continuidade de negócios.

Por fim, o Cobit fornece boas práticas através de um modelo de domínios e processos e apresenta atividades em uma estrutura lógica e gerenciável. As boas práticas do CobiT representam o consenso de especialistas. Elas são fortemente focadas mais nos controles e menos na execução. Essas práticas irão ajudar a otimizar os investimentos em TI, assegurar a entrega dos serviços e prover métricas para julgar quando as coisas saem erradas.

Na fase de execução do levantamento, os órgãos e entidades selecionados receberam, por meio de correspondência oficial, a identificação e a senha individual para

acesso ao questionário e, posteriormente, via mensagem eletrônica, o link para o questionário on-line. O software *Risk Manager* apoiou o envio, a coleta e a tabulação das informações do questionário. Durante o preenchimento do questionário, foi solicitado aos gestores de TI dos órgãos e entidades que anexassem documentos eletrônicos para servirem de evidências às respostas apresentadas. Ressalta-se, porém, que nesse primeiro momento, não foi avaliada a pertinência e a qualidade dos documentos produzidos e anexados.

Como limitação à execução dos trabalhos, deve-se destacar que alguns órgãos/entidades não dispunham de todas as informações solicitadas e fizeram muito esforço para obtê-las. Mesmo assim, alguns órgãos/entidades não conseguiram obter todas as informações e as questões relativas a elas ficaram sem resposta.

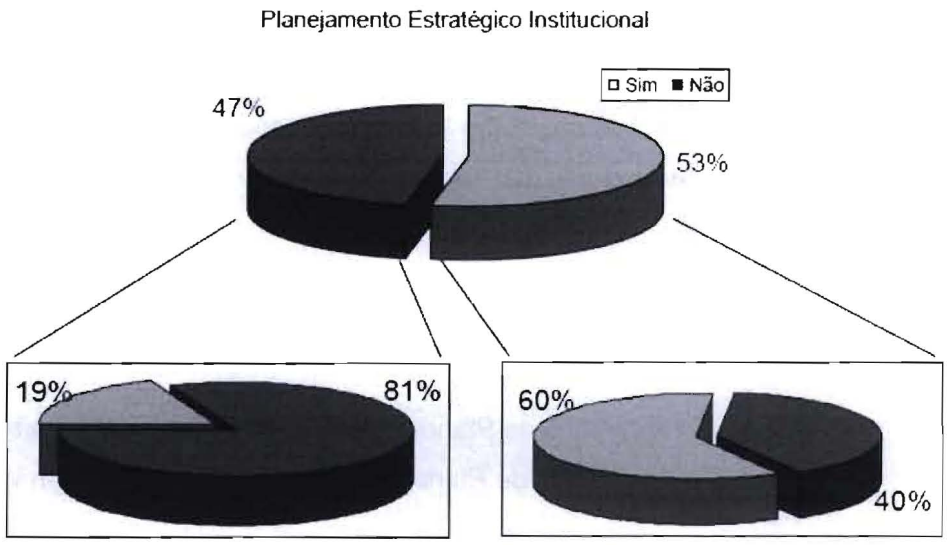
A partir dos próximos tópicos, serão apresentados os resultados obtidos pelo Tribunal de Contas da União, os critérios utilizados e os riscos decorrentes da falta de controles relativos à Governança de Tecnologia da Informação.

3.1.1. Planejamento estratégico institucional e de TI

De acordo com as informações coletadas pelo TCU, dos 255 órgãos/entidades pesquisados, 47% não tinham planejamento estratégico institucional em vigor. Dessa forma, ficou demonstrado que quase metade das organizações pesquisadas não possuíam a cultura de planejar suas ações de forma estratégica, apenas reagindo às demandas e mudanças ocorridas nos respectivos âmbitos de atuação.

Constatou-se, também, que 59% das organizações pesquisadas não faziam o planejamento estratégico de TI. Dessa forma, por meio de análises, o Tribunal percebeu que dos 47% dos órgãos/entidades que afirmaram não possuir planejamento estratégico institucional, 81%, isto é, 97 organizações não possuem planejamento estratégico de TI. Essa constatação pode ser observada através da análise do Gráfico 1 abaixo.

Gráfico 1 - Planejamento Estratégico



Planejamento Estratégico de TI

Fonte: Acórdão n.° 1.603/2008 - Tribunal de Contas da União

Deve-se ressaltar a importância do planejamento estratégico institucional (ou planejamento estratégico de negócio) e do planejamento estratégico de TI: o primeiro trata dos assuntos mais estratégicos da organização, assuntos relacionados à existência da organização, isto é, os principais objetivos desta, seus projetos mais importantes, as metas em longo prazo, os investimentos financeiros e de pessoal que serão feitos etc. Assim sendo, percebe-se que este planejamento é basilar, ou seja, todos os outros planos e ações devem ser elaborados e executados com o objetivo principal de atender ao que foi estabelecido no planejamento estratégico institucional. Por sua vez, o planejamento estratégico de TI, de acordo com Fernandes e Abreu (2012, p. 19), deve contemplar:

- Princípios de TI;
- Arquitetura de TI;
- Infraestrutura de TI;
- Necessidades de aplicações;
- Objetivos de desempenho e níveis de serviço e metas;
- Capacidade requerida de atendimento em relação a recursos humanos e infraestrutura;
- Organização das operações de serviços de TI;
- Estratégia para fornecedores de serviços;
- Competências requeridas;
- Políticas de segurança da informação;

- Investimentos e custeio;
- *Roadmap* de TI.

Assim, verifica-se que o planejamento estratégico de TI é de suma importância para esta área, visto que disporá sobre como a área de tecnologia da informação atenderá, em longo prazo, o planejamento estratégico institucional.

Com essas informações, o Tribunal de Contas da União elaborou os dois primeiros achados do levantamento:

- Achado I - Ausência de Planejamento estratégico institucional em vigor;
- Achado II - Ausência de Planejamento estratégico de TI em vigor.

Como critérios para o primeiro achado foram utilizados:

a) Cobit 4.1 PO1.2 Business-IT Alignment (Alinhamento de TI com negócio – Estabelecer processos de educação bidirecional e de envolvimento recíproco no planejamento estratégico para obtenção de alinhamento e integração entre o negócio e as ações de TI. As prioridades devem ser acordadas mutuamente a partir da negociação das necessidades do negócio e da área de TI);
b) Acórdão 1.558/2003-TCU-Plenário, item 9.3.9.

Os efeitos potenciais para este achado são:

a) Suporte ineficaz da área de TI na consecução da missão da organização;
b) Decisões dos gestores de TI incompatíveis com as necessidades da organização;
c) Alocação indevida de recursos de TI por falta de entendimento sobre as prioridades da organização;
d) Desperdício de recursos devido a decisões erradas acerca da alocação de recursos de TI.

Como critérios para o segundo achado foram utilizados:

a) Cobit 4.1 PO1.4 IT Strategic Plan (Plano Estratégico de TI – Criar um plano estratégico que defina, em cooperação com os principais interessados, como as metas de TI contribuirão para os objetivos estratégicos da organização e quais os custos e riscos associados. O plano deve incluir os serviços de TI, os ativos de TI e

como a área de TI dará suporte aos projetos dependentes de tecnologia da informação. A área de TI deve definir como os objetivos serão alcançados, as métricas a serem usadas e os procedimentos para obter a aprovação formal dos interessados. O plano estratégico de TI deve conter orçamento para investimentos e custeio de TI, fontes de recursos, estratégia de aquisições, e requisitos legais e regulatórios. O plano estratégico deve ser suficientemente detalhado para permitir a definição de planos táticos de TI);

b) Acórdão 1.558/2003-TCU-Plenário, item 9.3.9.

Os efeitos potenciais para este achado são:

a) Suporte ineficaz da área de TI na consecução da missão da organização;
b) Planos de TI não alinhados às necessidades do negócio;
c) Inexistência de consultas regulares entre gerente de TI e demais gerentes acerca dos projetos e serviços de TI;
d) Enfraquecimento das ações de TI;
e) Descontinuidade dos projetos de TI;
f) Insatisfação dos usuários;
g) Visão negativa da área de TI;
h) Resultados da área de TI abaixo do esperado;
i) Dificuldade de obtenção de recursos para a área de TI;
j) Investimentos desnecessários em TI;
k) Desperdício de recursos.

O Tribunal também constatou que menos de um terço (32%) dos órgãos/entidades pesquisados declararam possuir um comitê diretivo de TI ou algo equivalente. Dessa forma, segundo a Corte de Contas, por não haver um fórum competente para discussão, as decisões sobre investimentos em TI correm maior risco de serem equivocadas e levarem ao desperdício de recursos e, ainda, de não estarem alinhadas aos objetivos da organização.

Assim, o TCU elaborou o terceiro achado do levantamento:

- Achado III - Ausência de comitê diretivo sobre ações e investimentos em TI

Como critérios para o terceiro achado, foram utilizados:

a) Cobit 4.1 PO4.3 IT Steering Committee (Comitê Diretivo de TI – Criar um comitê diretivo de TI (ou equivalente) composto de gerentes executivos, de negócios e de TI, para: determinar as prioridades de investimento e alocação de recursos nas ações de TI, alinhadas às estratégias e prioridades da organização; acompanhar o estágio de desenvolvimento dos projetos e resolver conflitos relativos a recursos; e monitorar os níveis de serviço de TI e suas melhorias).

Os efeitos potenciais para este achado são:

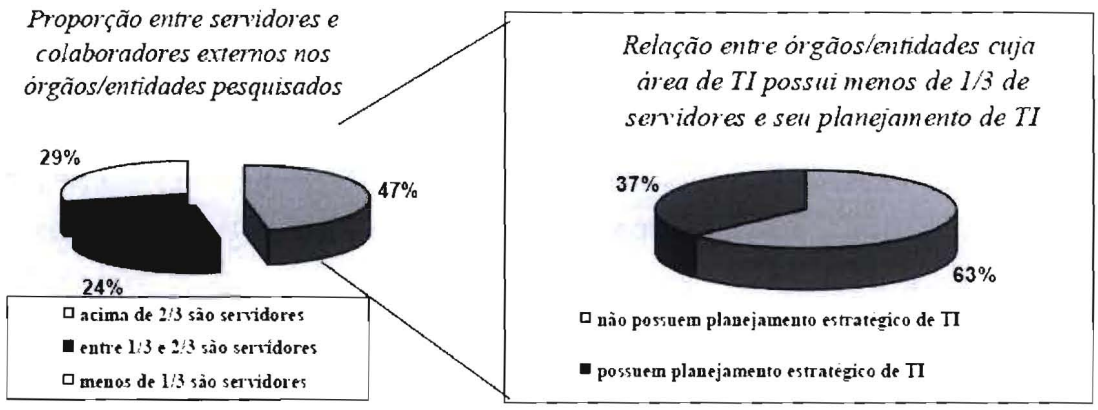
a) Estratégia de TI não alinhada com a estratégia da organização;
b) Apoio inexistente ou insuficiente dos projetos baseados em TI aos objetivos institucionais;
c) Apoio e envolvimento insuficientes da administração nas decisões essenciais da área de TI.

3.1.2. Estrutura de pessoal de TI

De acordo com os dados do levantamento, 95% dos órgãos/entidades informaram que possuem algum servidor do seu quadro atuando na área de TI. Contudo, ao verificar a proporção entre servidores do quadro e colaboradores externos a ele, foi possível observar ainda a ocorrência de muitos colaboradores externos em alguns órgãos/ entidades. O TCU considerou como colaboradores externos: requisitados com vínculo com a Administração Pública Federal; requisitados sem vínculo com a Administração Pública Federal (com ou sem comissão); terceirizados que atuam nas instalações físicas do órgão/entidade.

O Gráfico 2 mostra três grupos de órgãos/entidades: aqueles com mais de 2/3 do seu quadro composto por servidores, aqueles nos quais esse valor está entre 1/3 e 2/3, e aqueles onde os servidores constituem menos de 1/3 do quadro.

Gráfico 2 - Servidores/terceirizados na área de TI



Fonte: Acórdão n.° 1.603/2008 - Tribunal de Contas da União

Verificou-se que dentre os 70 órgãos pesquisados (29%), com área de TI composta de menos de ⅓ de servidores do quadro, 63% também não tinham planejamento estratégico de TI (Gráfico acima). Segundo o TCU, "ao mesmo tempo em que aumenta o risco de ausência de controles, a ausência de planejamento aponta uma potencial dificuldade de alocação de recursos humanos necessários à realização das ações de TI".

O Tribunal de Contas da União expressou preocupação com essa situação ao dispor que "a maior quantidade de colaboradores externos ao quadro dos órgãos/entidades pesquisados aumenta o risco de perda de conhecimento organizacional, na medida em que esse conhecimento esteja depositado em indivíduos sem vínculo e menos compromissados com a organização. Quanto menor o quadro de servidores, maior a probabilidade de que algum conhecimento fique somente entre os colaboradores externos e, portanto, maior o risco de que esse conhecimento se perca".

Segundo o levantamento, somente 37% dos servidores que atuavam nas áreas de TI dos órgãos/entidades pesquisados possuíam formação específica em TI (incluindo aqui doutorado, mestrado, pós-graduação *lato sensu* e nível superior).

De acordo com a Corte, "a falta de especialização preocupa em função do aumento da importância estratégica da TI para as organizações, pois um quadro menos especializado tende a produzir resultados de mais baixa qualidade. Outra preocupação é que tal perfil leve a organização a buscar no mercado a competência pessoal que lhe falta em seu quadro, seja por meio de terceirizados, seja por meio de requisições/comissões".

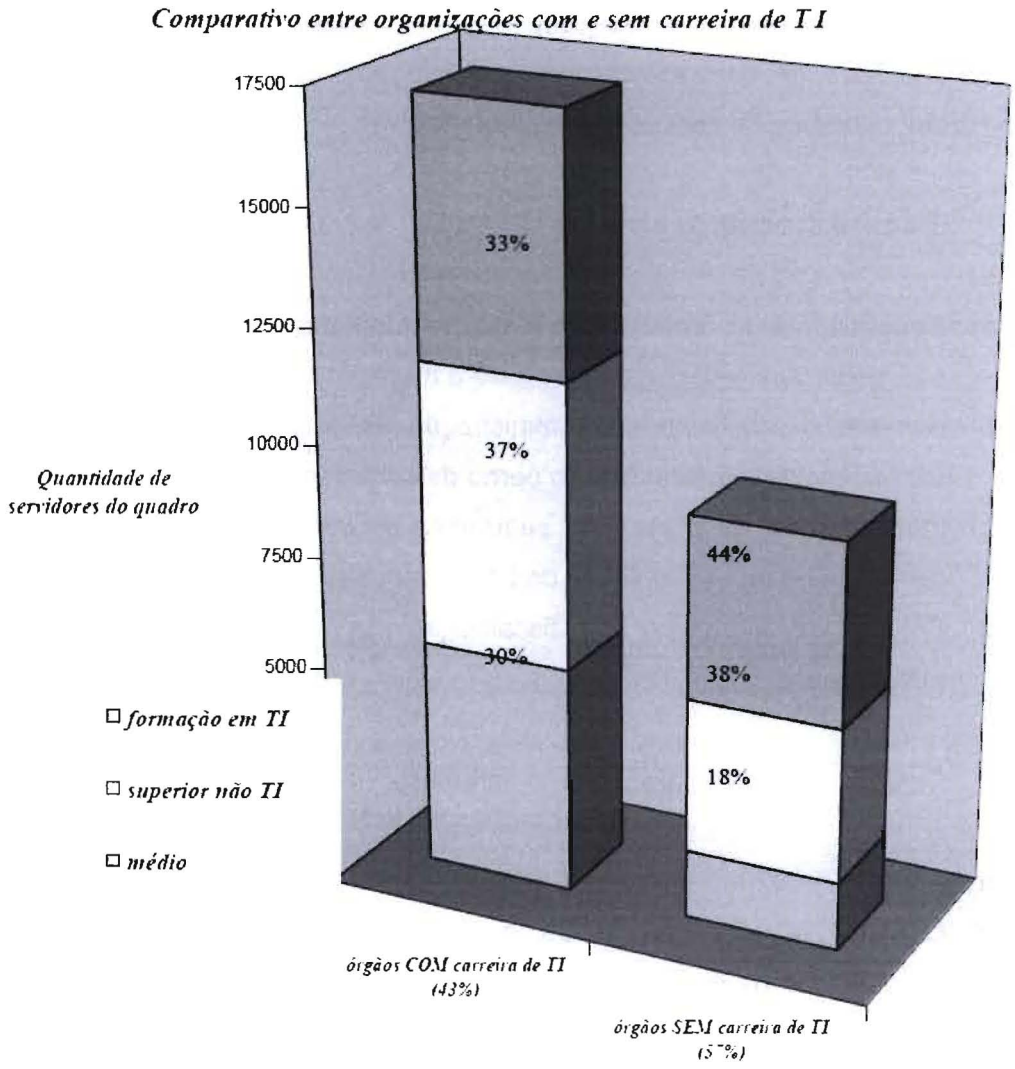
Comprovando a preocupação do TCU, percebeu-se que entre os colaboradores requisitados/comissionados há um percentual maior (48%) com formação específica em TI.

Além do mais, um total de 60% dos pesquisados declarou que não consideravam as competências gerenciais, técnicas e resultados produzidos anteriormente na seleção de pessoas para funções comissionadas na área de TI. O risco nesse caso, segundo o TCU, é uma baixa qualificação do corpo gerencial de TI e o comprometimento dos resultados da área, desde a falta de alinhamento com os negócios até a perda de produtividade da equipe por má gestão.

Por fim, um total de 57% dos pesquisados informou que não possui carreira específica para a área de TI. Segundo os dados, os 43% dos órgãos/entidades que têm carreira de TI possuem ⅔ do total de pessoal alocado para TI entre os pesquisados.

De acordo com o levantamento, em valores absolutos, há mais profissionais com formação em TI (incluindo doutorado, mestrado, pós-graduação lato sensu e nível superior) nas organizações com carreira específica: 58% dos profissionais com formação em TI estão nessas organizações. Contudo, há que se registrar que, em valores proporcionais, não há diferença significativa entre a formação em TI dos servidores em órgãos com e sem carreira específica (37% e 38% respectivamente – Gráfico 3). Ou seja, mesmo nos órgãos com carreira específica, ainda há muitos servidores sem formação superior em TI ou com formação em nível médio.

Gráfico 3 - Formação dos profissionais de TI



Fonte: Acórdão n.° 1.603/2008 - Tribunal de Contas da União

Com essas informações, o Tribunal de Contas da União elaborou outros quatro achados do levantamento:

- Achado IV - Quantidade reduzida de servidores na área de TI;
- Achado V - Ausência de formação específica em TI;
- Achado VI - Inobservância das competências necessárias para funções comissionadas;
- Achado VII - Ausência de carreira específica para a área de TI.

Foram utilizados como critérios para o quarto achado:

a) Acórdão 140/2005–TCU–Plenário;
b) Cobit 4.1 PO7.5 Dependence Upon Individuals (Dependência em Indivíduos – Minimizar a ocorrência de dependência crítica em indivíduos chave por meio de aquisição de conhecimento (documentação), compartilhamento de conhecimento, planejamento de sucessão e equipe reserva).

Efeitos potenciais do achado:

a) Dependência do órgão/entidade de servidores/empregados alheios ao quadro para execução de atividades críticas para o negócio;
b) Aumento de custo para a Administração em contratos onde o contratado não pode ser facilmente substituído sem perda de continuidade de serviços de TI;
c) Inobservância da política de segurança da informação da empresa em função da necessidade de manipulação de informações sigilosas por terceirizados;
d) Conflito de interesses na fiscalização de contratos, quando feita por outros terceirizados.

Critérios utilizados para o quinto achado:

a) Acórdão 140/2005–Plenário;
b) Cobit 4.1 PO7.2 Personnel Competencies (Competências Pessoais – Regularmente verificar que os profissionais de TI têm as competências necessárias para exercer sua função com base em sua formação, treinamento e/ou experiência. Definir as competências de TI básicas e verificar que são mantidas, por meio de programas de qualificação e certificação quando apropriados).

Efeitos potenciais do achado:

a) Baixa qualidade dos serviços de TI em função da baixa qualificação da equipe de TI;
b) Órgão/entidade dependente de prestadora de serviços de TI.

Critérios utilizados para o sexto achado:

a) Decreto no 5.707, de 23 de fevereiro de 2006, art. 3o, incisos VI e VII.

Efeitos potenciais do achado:

a) Baixa produtividade da equipe de TI em função da baixa qualidade do corpo gerencial;
b) Falta de alinhamento da TI com o negócio da organização.

Critérios utilizados para o sétimo achado:

a) Cobit 4.1 PO7.1 Personnel Recruitment and Retention (Recrutamento e Retenção de Pessoal – Manter processos de recrutamento de pessoal de TI em linha com as políticas e os procedimentos de pessoal gerais da organização, isto é, contratação, ambiente positivo para o trabalho, orientação. Implementar processos que garantam que a organização tenha força de trabalho de TI apropriadamente preparada com as habilidades necessárias para atingir os objetivos organizacionais).

Efeitos potenciais do achado:

a) Insuficiência de servidores para atuar na área de TI.

3.1.3. Segurança da informação

Segundo o levantamento de informações, a ausência de política de segurança da informação (PSI) formalmente definida na organização foi declarada por 64% dos órgãos/entidades pesquisados. De acordo com o TCU, "como esse documento de diretrizes é um dos primeiros passos na construção de uma gestão da segurança da informação, tal achado é um indício preocupante de que essa gestão é inexistente ou incipiente na maioria das organizações da Administração Pública Federal".

O Tribunal também constatou que a cultura de segurança da informação predominante nas organizações brasileiras, inclusive na área governamental, ainda não estava madura o suficiente no que diz respeito à preocupação com desastres e interrupção nos serviços. É o que se viu da ausência de plano de continuidade de negócios (PCN) em cerca de 88% dos pesquisados. A situação se agravou quando, adicionalmente, observou-se que, dentre os que possuem PCN em vigor, apenas 30% declararam tê-lo revisado em período inferior a um ano.

De acordo com o TCU, "a ausência de PCN na organização é um indício de falta de conscientização em nível estratégico com os riscos de interrupção dos serviços da

organização. Sem planejamento dessa natureza, a organização fica vulnerável quando da ocorrência de desastres (naturais ou por sabotagem) e interrupções de serviços. Eventos que poderiam ser resolvidos sem grande perda, acabam por comprometer toda a base atual e histórica de informações da organização. Pode ser até que o PCN nunca precise ser acionado mas, se houver a necessidade e ele não existir, isso pode significar risco à continuidade da existência da organização".

Verificou-se também que 80% dos órgãos/entidades declararam não classificar as informações. Segundo a Corte de Contas, "a classificação das informações, porém, de forma semelhante à PSI, é um dos pilares da segurança da informação numa organização. A sua ausência indica que o tratamento da segurança sobre as informações não é feito de forma consistente, variando em função da maior ou menor maturidade das áreas que as armazenam, transportam ou alteram. Assim, pode ser, por exemplo, que uma informação em papel seja tratada com um nível maior de sigilo, mas ao ser passada para um sistema informatizado, receba o tratamento comum dado a outras informações não-sigilosas, inadequado para suas especificidades. Como não existe um rótulo de segurança único para aquela informação, o qual deveria apontar para procedimentos próprios em cada meio de armazenamento, o tratamento da segurança daquela informação torna-se ineficaz como um todo, já que é uma máxima da segurança da informação que a segurança de um conjunto é igual à segurança do elo mais fraco".

De acordo com as respostas fornecidas, procedimentos para disciplinar o controle de acesso a recursos computacionais existem em 52% dos pesquisados. O TCU dispõe que "é provável que esse resultado seja uma consequência da necessidade de controle de acesso lógico em sistemas de informação e sistemas operacionais em geral, que induz a necessidade de definição de normativos de identificação e de senhas, bem como de direitos de acesso para cada usuário ou grupo de usuários Isso faz com que a situação dos 48% restantes seja crítica".

Um total de 64% dos órgãos/entidades informou que não possuíam área específica, com responsabilidades definidas, para lidar estrategicamente com segurança da informação. De acordo com o Tribunal, "sem tal estrutura, há grande probabilidade de que as questões de segurança não sejam tratadas de maneira consistente. Além disso, torna-se difícil para a organização avaliar se estão sendo endereçados de modo adequado os recursos humanos e de logística para a implementação dos controles de segurança da informação, ou se tais controles estão sintonizados com o negócio da organização. A ausência de fórum adequado, de nível estratégico e com representantes de diversas áreas da organização,

também é um indício de ausência de um fator considerado crítico no sucesso da gestão da segurança: a preocupação da direção da organização com a segurança da informação".

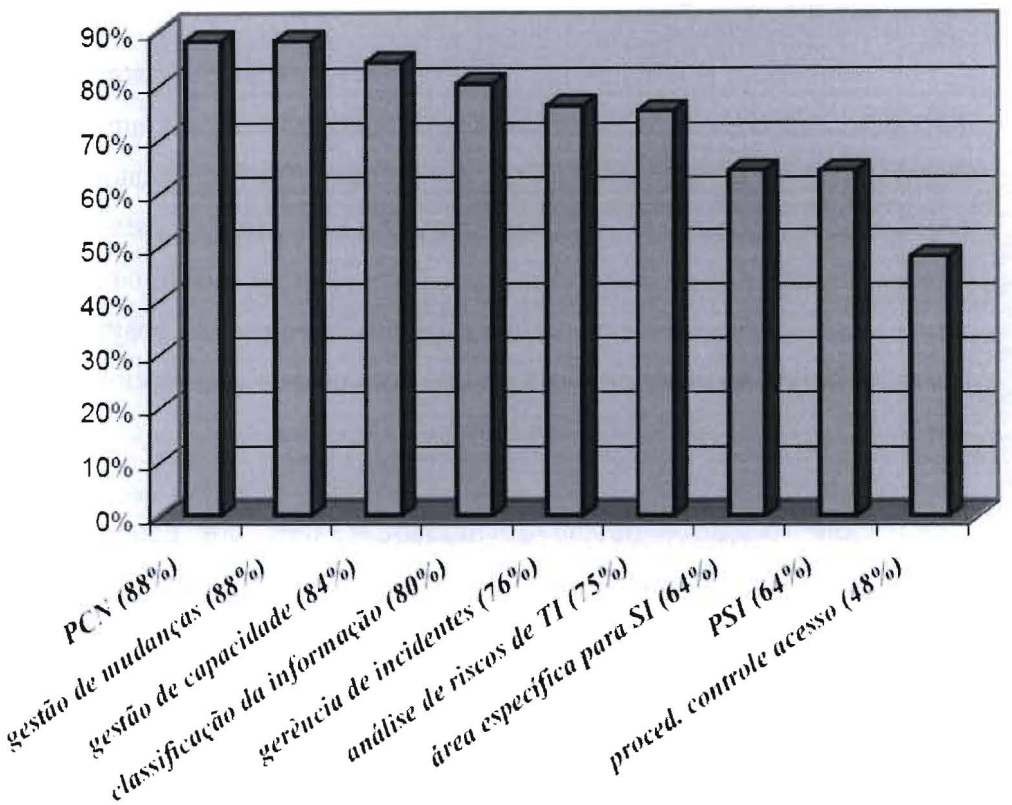
Segundo o levantamento, não existe área específica para gerência de incidentes em 76% dos órgãos/entidades pesquisados. Adicionalmente, em outra questão verificou-se que, coincidentemente, apesar de não serem as mesmas instituições, também 76% das organizações pesquisadas oferecem serviços transacionais pela Internet, o que aumenta a sua exposição a tentativas de acesso indevido e à indisponibilidade da informação. Ao cruzar esses dados, verificou-se que 54% dos pesquisados possuem serviços transacionais pela Internet e não possuem área própria para gerência de incidentes. Nesses casos, o risco associado à ausência do controle aumenta.

Com relação à gestão de mudanças, 88% dos pesquisados declarou que não gerenciam mudanças. Sabe-se que mudanças no ambiente de TI, sem o devido controle, são causas comuns de instabilidade e falhas de segurança.

De acordo com as respostas recebidas, a gestão de capacidade e compatibilidade não é feita em 84% dos órgãos/entidades pesquisados. Tal processo está ligado ao monitoramento do ambiente de TI e sua ausência indica que esse monitoramento não é executado adequadamente. A principal consequência, segundo o TCU, é o aumento do risco de descontinuidade na prestação dos serviços de TI, o que afeta diretamente a disponibilidade das informações.

Por fim, em 75% dos órgãos/entidades pesquisados não há análise de riscos na área de TI. De acordo com a Corte de Contas, "é um indício de que as ações de segurança não são executadas de maneira sintonizada com as necessidades do negócio dessas organizações. Isto porque, sem análise de riscos, não há como o gestor priorizar ações e investimentos com base em critérios claros e relacionados com o negócio da organização. O resultado pode ser desperdício, uso ineficaz de recursos, carência de ações prioritárias".

Gráfico 4 - Deficiências na segurança da informação



Fonte: Acórdão n.° 1.603/2008 - Tribunal de Contas da União

Com essas informações, o Tribunal de Contas da União elaborou achados do levantamento:

- Achado VIII - Ausência de política de segurança da informação;
- Achado IX - Ausência de plano de continuidade de negócios em vigor;
- Achado X - Ausência de classificação das informações;
- Achado XI - Ausência de procedimentos de controle de acesso em vigor;
- Achado XII - Ausência de área específica para lidar com segurança da informação;
- Achado XIII - Ausência de área específica para gerência de incidentes;
- Achado XIV - Ausência de gestão de mudanças;
- Achado XV - Ausência de gestão de capacidade e compatibilidade das soluções de TI;
- Achado XVI - Ausência de análise de riscos na área de TI.

Foram critérios para o oitavo achado:

a) NBR ISO/IEC 17799:2005, item 5.1 – Política de segurança da informação: convém que a direção estabeleça uma política clara, alinhada com os objetivos do negócio e demonstre apoio e comprometimento com a segurança da informação por meio da publicação e manutenção de uma política de segurança da informação para toda a organização;
b) Cobit 4.1 DS5.2 IT Security Plan (Plano de Segurança de TI – Traduzir requisitos de negócio, risco e conformidade num plano geral de segurança de TI, levando em consideração a infra-estrutura de TI e a cultura de segurança. Garantir que o plano seja implementado dentro das políticas e dos procedimentos de segurança em conjunto com investimentos apropriados em serviços, pessoal, software e hardware. Comunicar as políticas e procedimentos de segurança aos interessados e usuários).

Efeitos potenciais deste achado:

a) Enfraquecimento das ações de segurança, por não serem respaldadas por uma política institucional;
b) Descompasso entre a gestão da segurança da informação e os objetivos de negócio;
c) Percepção pelos usuários e clientes de falta de comprometimento da alta administração da organização com a segurança da informação.

Critérios para o nono achado:

a) NBR 15999-1:2007, item 8.6 – Planos de Continuidade de Negócios: o propósito de um plano de continuidade de negócios (PCN) é permitir que uma organização recupere ou mantenha suas atividades em caso de uma interrupção das operações normais de negócios.
b) Cobit 4.1 DS4 Ensure Continuous Service (Garantir a Continuidade do Serviço – A necessidade de prover serviços contínuos de TI requer desenvolvimento, manutenção e teste de planos de continuidade de TI, armazenamento de cópias de segurança em local alternativo e treinamento periódico de planejamento de continuidade).
c) NBR ISO/IEC 17799:2005, item 14.1.3 – Desenvolvimento e implementação de planos de continuidade relativos à segurança da informação: convém que os planos sejam desenvolvidos e implementados para a manutenção ou recuperação das operações e para assegurar a disponibilidade da informação no nível requerido e na escala de tempo requerida, após a ocorrência de interrupções ou falhas dos processos críticos do negócio.

Efeitos reais e potenciais deste achado:

a) Vulnerabilidade das organizações à ocorrência de desastres e interrupção de serviços;
b) Perda de dados, inclusive históricos, de difícil recuperação;
c) Dificuldade no restabelecimento das operações normais quando da ocorrência de interrupção de serviços;
d) Vulnerabilidade a fraudes e erros durante a interrupção de serviços;
e) Paralisação de funções essenciais de governo e/ou de Estado.

Critérios para o décimo achado:

a) Cobit 4.1 PO2.3 Data Classification Scheme (Esquema de Classificação da Informação – Estabelecer um esquema de classificação aplicável em toda organização baseado na criticidade e na sensibilidade – isto é, pública, reservada ou sigilosa – das informações institucionais. Esse esquema deve incluir detalhes sobre propriedade da informação; definição de níveis de segurança e controles de proteção adequados; e uma breve descrição dos requisitos de retenção e destruição de dados, criticidade e sensibilidade. Deve ser usado como a base para a aplicação de controles tais como controles de acesso, armazenamento ou encriptação);
b) NBR ISO/IEC 17799:2005, item 7.2 – Classificação da informação: convém que a informação seja classificada para indicar a necessidade, prioridades e o nível esperado de proteção quando do tratamento da informação.

Efeitos potenciais deste achado:

a) Informações tratadas com nível inadequado de proteção, suscetíveis à perda de integridade, confiabilidade e disponibilidade;
b) Tratamento da segurança das informações de maneira inconsistente e dependente do meio em que transitam ou são armazenadas;
c) Falta de amparo para responsabilização por acesso indevido a informações;
d) Falta de sintonia entre a proteção das informações e o negócio da organização.

Critérios para o décimo primeiro achado:

a) Cobit 4.1 DS5.3 Identity Management (Gerência de Identidade – Garantir que todos usuários (internos, externos e temporários) e sua atividade em sistemas de TI (aplicações do negócio, sistema operacional, desenvolvimento e manutenção) devem ser unicamente identificáveis. Direitos de acesso do usuário a sistemas e dados devem estar alinhados com as necessidades do negócio e requisitos do cargo definidos e documentados. Direitos de acesso do usuário são requisitados pelo gerente do usuário, aprovados pelo proprietário do sistema e implementados pelo responsável pela segurança. Identidades e direitos de acesso do usuário são mantidos num repositório central. Medidas técnicas e procedimentais são alocadas e mantidas correntes para estabelecer identificação do usuário, implementar autenticação e conceder os direitos de acesso);
b) Cobit 4.1 DS5.4 User Account Management (Gerência de Contas de Usuários – Garantir que requisitar, estabelecer, entregar, suspender, modificar e fechar contas de usuários e respectivos privilégios de usuário é realizado pela gerência de contas de usuário. Deve ser incluído um procedimento de aprovação pelo proprietário do sistema ou dado delineando a concessão de privilégios de acesso. Esses procedimentos devem ser aplicados para todos usuários, incluindo administradores (usuários privilegiados), usuários internos e externos, em uso normal ou em casos de emergência. Direitos e obrigações relativos a acessos a sistemas e dados corporativos são contratualmente ajustados para todos os tipos de usuários. Executar revisão regular gerencial de todas as contas e respectivos privilégios.
c) Cobit 4.1 DS12.2 Physical Security Measures (Medidas de Segurança Física – Definir e implementar medidas de segurança física alinhadas com os requisitos do negócio para assegurar o local e os ativos físicos. Medidas de segurança física devem ser capazes de eficientemente prevenir, detectar e mitigar riscos relativos a roubos, temperatura, incêndio, fumaça, água, tremor de terra, terrorismo, vandalismo, interrupções de energia, produtos químicos ou explosivos);
d) Cobit 4.1 DS12.3 Physical Access (Acesso Físico – Definir e implementar procedimentos para permitir, limitar e revogar acesso aos terrenos, edifícios e áreas de acordo com as necessidades do negócio, inclusive emergências. Acesso aos terrenos, edifícios e áreas deve ser justificado, autorizado, registrado e monitorado. Isso deve ser aplicado a todas as pessoas que entrem na propriedade, incluindo funcionários, terrporários, clientes, vendedores, visitantes ou qualquer outro terceiro);
e) NBR ISO/IEC 17799:2005, item 11.1.1 – Política de controle de acesso: convém que a política de controle de acesso seja estabelecida, documentada e analisada

criticamente, tomando-se como base os requisitos de acesso dos negócios e segurança da informação.

Efeitos potenciais deste achado:

a) Perfil de acesso a informações excessivamente permissivo para determinados usuários ou grupos de usuários;
b) Concessão ou alteração do acesso a recurso para pessoas não autorizadas, visando fraudes;
c) Divulgação não autorizada de informação reservada ou sigilosa.

Critérios para o décimo segundo achado:

a) Cobit 4.1 DS5.1 Management of IT Security (Gerência da Segurança de TI – Gerenciar a segurança de TI no nível organizacional apropriado mais alto de maneira que a gerência de ações de segurança esteja alinhada com os requisitos do negócio);
b) NBR ISO/IEC 17799:2005, item 6.1 – Infra-estrutura da segurança da informação: convém que uma estrutura de gerenciamento seja estabelecida para iniciar e controlar a implementação da segurança da informação dentro da organização.

Efeitos potenciais deste achado:

a) Ausência ou atuação deficiente em segurança da informação na organização;
b) Ações de segurança da informação da organização incoerentes e ineficazes;
c) Desperdício de recursos em ações não-prioritárias.

Critérios para o décimo terceiro achado:

a) Cobit 4.1 DS5.5 Security Testing, Surveillance and Monitoring (Teste, Vigilância e Monitoramento de Segurança – Testar e monitorar a implementação da segurança de TI de uma forma proativa. A segurança de TI deve ser formalmente aprovada de uma maneira tempestiva para assegurar a manutenção do padrão estabelecido de segurança da informação da organização. A função de registro e monitoramento permitirá a prevenção e/ou rápida detecção e o subsequente informe tempestivo de atividades não usuais e/ou anormais que necessitem de tratamento);

b) Cobit 4.1 DS5.6 Security Incident Definition (Definição de Incidente de Segurança – Definir e comunicar claramente as características de potenciais incidentes de segurança para que possam ser corretamente classificados e tratados pelo processo de gestão de problemas e incidentes);
c) NBR ISO/IEC 17799:2005, item 13.2 – Gestão de incidentes de segurança da informação e melhorias: convém que responsabilidades e procedimentos estejam definidos para o manuseio efetivo de eventos de segurança da informação e fragilidades, uma vez que estes tenham sido notificados. Convém que um processo de melhoria contínua seja aplicado às respostas, monitoramento, avaliação e gestão total de incidentes de segurança da informação.

Efeitos potenciais deste achado:

a) Tratamento de incidentes inexistente, inadequado ou inconsistente;
b) Inexistência de registro histórico de incidentes, o que dificulta o aprendizado e o tratamento das causas;
c) Maior risco de que indisponibilidades, perdas de integridade ou acessos indevidos tenham maior impacto sobre as informações e, consequentemente, sobre o negócio da organização.

Critérios para o décimo quarto achado:

a) Cobit 4.1 AI6 Manage Changes (Gestão de Mudanças – Todas as mudanças, incluindo manutenção e correções de emergência, relativas a infraestrutura e aplicativos do ambiente de produção, devem ser formalmente geridas de maneira controlada);
b) NBR ISO/IEC 17799:2005, item 10.1.2 – Gestão de mudanças: convém que modificações nos recursos de processamento da informação e sistemas sejam controladas;
c) NBR ISO/IEC 17799:2005, item 12.5.1 – Procedimentos para controle de mudanças: convém que a implementação de mudanças seja controlada utilizando procedimentos formais de controle de mudanças.

Efeitos potenciais deste achado:

a) Comprometimento da disponibilidade das informações nos sistemas e da estabilidade do ambiente de TI devido à realização de mudanças não-criteriosas;

b) Impossibilidade de restaurar uma situação anterior a uma mudança malsucedida, pela falta de cuidado com a preservação do estado anterior e de registro preciso dos passos executados;
c) Alteração do nível de proteção de uma ou várias informações de forma não avaliada, não prevista ou não aprovada pelo gestor da informação como efeito de mudança em um recurso de TI.

Critérios para o décimo quinto achado:

a) Cobit 4.1 PO3.4 Technology Standards (Padrões Tecnológicos – Para prover soluções tecnológicas consistentes, efetivas e seguras para toda a organização, estabelecer um fórum de tecnologia para prover diretrizes tecnológicas, pareceres e indicação sobre produtos de infraestrutura e seleção de tecnologias, e verificar a conformidade com esses padrões e diretrizes. Esse fórum deve direcionar as práticas e padrões tecnológicos com base na relevância para o negócio, riscos e conformidade com requisitos externos);
b) Cobit 4.1 DS3 Manage Performance and Capacity (Gestão de Capacidade e Desempenho – A necessidade de gerir a capacidade e o desempenho dos recursos de TI requer um processo de avaliação periódica do desempenho atual e da capacidade desses recursos. Esse processo inclui prever futuras necessidades com base na carga de trabalho e nos requisitos de armazenamento e de contingência. Esse processo garante que as fontes de informação que suportam os requisitos de negócio estejam continuamente disponíveis);
c) NBR ISO/IEC 17799:2005, item 10.3.1 – Gestão de capacidade: convém que a utilização dos recursos seja monitorada e sincronizada e as projeções feitas para necessidades de capacidade futura, para garantir o desempenho requerido do sistema.

Efeitos potenciais deste achado:

a) Interrupções nos sistemas de informação por sobrecarga no processamento e indisponibilidade das informações;
b) Inadequação de investimentos em infraestrutura de TI, por desconhecimento da real capacidade do ambiente e das necessidades de ampliação/atualização;
c) Desperdício provocado pela aquisição de produtos de TI incompatíveis com o ambiente existente.

Critérios para o décimo sexto achado:

a) Cobit 4.1 PO9.4 Risk Assessment (Análise de Riscos – Avaliar periodicamente a probabilidade e o impacto de todos os riscos identificados, usando métodos qualitativos e quantitativos. A probabilidade e o impacto associados com o risco inerente e residual devem ser determinados individualmente por categoria);
b) NBR ISO/IEC 17799:2005, item 4.1 – Analisando/avaliando os riscos de segurança da informação: convém que as análises/avaliações de riscos identifiquem, quantifiquem e priorizem os riscos com base em critérios relevantes para a organização, e que os resultados orientem e determinem as ações de gestão apropriadas e as prioridades para o gerenciamento dos riscos de segurança da informação, e para a implementação dos controles selecionados, de maneira a proteger contra estes riscos.

Efeitos potenciais deste achado:

a) Estabelecimento inadequado de prioridades para ações de segurança;
b) Desperdício de recursos em ações não-prioritárias, enquanto outras mais críticas deixam de ser realizadas.

3.1.4. Desenvolvimento de sistemas de informação

Segundo informações fornecidas, o TCU constatou que é adotada uma metodologia de desenvolvimento de sistemas em quase metade dos pesquisados (49%). De acordo com o Tribunal "a ausência de metodologia em 51% dos pesquisados aumenta o risco de construir sistemas pouco robustos, suscetíveis a falhas, sem testes adequados e com documentação deficiente, ou seja, aumenta o risco de que etapas mal conduzidas do processo produzam resultados inadequados para a organização. Um levantamento malfeito, por exemplo, gera um produto que não é o esperado pelo cliente; um sistema mal documentado ou cuja documentação não segue um padrão ou, ainda, cuja documentação não é atualizada corretamente, fica dependente da manutenção pelo(s) desenvolvedor(es); um teste mal realizado permite que programas não adequadamente homologados pelo cliente sejam dados como concluídos".

Além disso, segundo o levantamento realizado, o risco para a organização é ainda maior quando se verifica que, dentre os 130 pesquisados que declararam não ter

metodologia, 68% informaram que ofereciam serviço transacional pela Internet e, portanto, possuíam sistemas expostos a ações indevidas, intencionais ou não. Segundo o Tribunal, "tal exposição é significativa pois, na Internet brasileira, os ataques a servidores web no primeiro trimestre de 2008 aumentaram 34% em relação ao trimestre anterior, e 519% em relação ao mesmo período de 2007 (Estatísticas do CERT.br para o primeiro trimestre de 2008)".

O Tribunal ainda dispõe que "sem uma metodologia, não é possível terceirizar todo o processo de desenvolvimento ou mesmo parte dele sem que isso represente um risco para a organização. Como o processo em si não é bem definido, não há como medir o serviço prestado ou garantir que não haverá perda de conhecimento ou ainda que o resultado seja o adequado para a organização".

Com essas informações, o Tribunal elaborou o achado VXII: Não-adoção de metodologia de desenvolvimento de sistemas.

Como critérios para este achado foram utilizados:

a) Cobit 4.1 AI2.7 Development of Application Software (Desenvolvimento de Software Aplicativo – Assegurar que os aplicativos sejam desenvolvidos de acordo com as especificações de projeto, padrões de desenvolvimento e documentação, requisitos de qualidade e padrões de aprovação. Assegurar que todos os aspectos legais e contratuais estejam identificados e tratados para software aplicativo desenvolvido por terceiros).

Efeitos potenciais deste achado:

a) Processo de desenvolvimento de sistemas lento e sistemas de informação ineficazes;
b) Perda de informações por causa de sistemas pouco robustos, sujeitos a falhas de segurança, seja por fraude, seja por uso incorreto;
c) Execução de contratos de prestação de serviços de desenvolvimento sem métricas adequadas nem etapas claras com produtos para cada etapa;
d) Sistemas de difícil manutenção, sem documentação, em que apenas quem desenvolveu detém o conhecimento. Esse caso pode ser ainda mais sério se o desenvolvedor for contratado externamente.

3.1.5. Gestão de acordos de níveis de serviço

De acordo com a Corte de Contas, a gestão de níveis de serviços foi a questão com mais alto percentual de resposta negativa: 89% dos pesquisados informaram não executar a gestão de níveis de serviço de TI ofertados aos seus clientes.

Segundo o TCU, "a ausência da gestão de acordo de níveis de serviço em percentual tão expressivo indica que grande parte dos pesquisados não realiza a negociação da qualidade dos serviços de TI com os seus clientes. A consequência disso é uma dificuldade em ajustar expectativas: as áreas de TI não sabem se estão atendendo às necessidades de qualidade de serviço dos seus clientes, nem tampouco os clientes sabem, ao pedir um serviço de TI, qual o nível de qualidade que podem esperar. Os resultados podem ser áreas de TI cujos esforços e investimentos não estão sintonizados com as necessidades e expectativas dos seus clientes".

Constatou-se, também, que 74% dos pesquisados não executam a gestão de níveis de serviço dos serviços contratados, ou seja, mesmo quando o órgão/entidade é cliente e não fornecedor, não há preocupação com a avaliação e o controle dos resultados.

Dessa forma, o Tribunal elaborou mais dois achados:

- Achado XVIII - Ausência de gestão de acordos de níveis de serviços prestados internamente;
- Achado XIX - Ausência de gestão de acordos de níveis de serviços contratados externamente

Foram critérios para o décimo oitavo achado:

a) Cobit 4.1 DS1 Define and Manage Service Levels (Definir e Gerenciar Níveis de Serviço – A comunicação efetiva entre gerente de TI e usuários sobre requisitos de serviço é possível por meio de acordo definido e documentado acerca dos serviços de TI e níveis de serviço. Esse processo também inclui monitoramento e divulgação tempestiva aos interessados do cumprimento dos níveis de serviço. Esse processo permite um alinhamento entre os serviços de TI e os requisitos de negócio relacionados).

Efeitos potenciais deste achado:

a) Insatisfação dos clientes com a qualidade e desempenho das soluções ofertadas por sua área de TI;
b) Ausência de informações para os gerentes de TI sobre as reais expectativas dos seus clientes;
c) Inadequação da distribuição dos investimentos em TI em relação às necessidades dos clientes.

Foram critérios para o décimo nono achado:

a) Cobit 4.1 DS1 Define and Manage Service Levels (Definir e Gerenciar Níveis de Serviço – A comunicação efetiva entre gerente de TI e usuários sobre requisitos de serviço é possível por meio de acordo definido e documentado acerca dos serviços de TI e níveis de serviço. Esse processo também inclui monitoramento e divulgação tempestiva aos interessados do cumprimento dos níveis de serviço. Esse processo permite um alinhamento entre os serviços de TI e os requisitos de negócio relacionados).

Efeitos potenciais deste achado:

a) Insatisfação dos clientes com a qualidade e desempenho das soluções de TI contratadas;
b) Realização e manutenção de contratos de qualidade inadequada e pouco efetivos para o negócio da organização;
c) Inadequação da distribuição dos investimentos em TI em relação às necessidades da organização;
d) Não-aplicação de multas contratuais e pagamento de valores indevidos aos fornecedores.

3.1.6. Processo de contratação de bens e serviços de TI

O levantamento constatou que 54% dos órgãos/entidades pesquisados adotavam processo formal de trabalho para contratações de TI, porém, segundo o Tribunal, "a situação

está longe do ideal, já que um percentual expressivo de organizações (46%) não adota processo formal de trabalho para contratações".

De acordo com TCU, "deve-se observar que isso não significa deixar de cumprir a legislação específica. Entretanto, a falta de um processo de trabalho definido, padronizado, documentado e aprovado para realizar as contratações de TI pode trazer consequências danosas à organização. Como não existe um padrão oficial e disseminado pela organização, cada área pode adquirir os recursos de que necessita de uma forma diferente. Dessa maneira, a organização se expõe a riscos desnecessários e que poderiam ser evitados com a adoção de um processo de trabalho formalizado".

O item 9.4 do Acórdão 786/2006-TCU-Plenário recomendou à Secretaria de Logística e Tecnologia da Informação do Ministério do Planejamento, Orçamento e Gestão (SLTI) que elaborasse 'um modelo de licitação e contratação de serviços de informática para a Administração Pública Federal' e promovesse 'a implantação dele nos diversos órgãos e entidades sob sua coordenação mediante orientação normativa'. Em atendimento a esse acórdão, durante o processo de revisão do relatório do levantamento de informações, a SLTI publicou a Instrução Normativa n.º 4, de 19 de maio de 2008. A IN-4 da SLTI dispõe sobre o processo de contratação de serviços de TI pela Administração Pública Federal direta, autárquica e fundacional. A norma contempla as fases de planejamento da contratação, seleção do fornecedor e gerenciamento do contrato e entrou em vigor no dia 2 de janeiro de 2009.

Constatou-se, também, que pouco mais da metade (53%) dos órgãos/entidades pesquisados realiza a análise de custo/benefício da solução de TI contratada. Além do mais, 40% dos órgãos e entidades ainda não se preocupam em justificar e destacar os benefícios esperados para a organização.

O Tribunal Contas da União também percebeu, por parte dos pesquisados, a não-exigência de demonstrativo de formação de preço antes da adjudicação.

A Corte dispõe que "o valor de muitas contratações de TI é resultado da soma de valores de diversos componentes. Especialmente na contratação de uma solução de TI, os custos dos componentes podem variar ao longo do tempo de duração do contrato de maneira diferente. Tome-se como exemplo uma solução de TI que envolva recursos humanos, aluguel de equipamentos e recursos de telecomunicação. Pode ser necessário, para se manter o equilíbrio econômico-financeiro do contrato, que haja a repactuação com a

assinatura de termo aditivo por questões econômicas, de mercado ou tecnológicas. Se não se souber o quanto cada componente representa na formação do valor final, não se poderá repactuar o contrato de maneira justa e não lesiva aos interesses públicos".

Com base nessas informações, O TCU elaborou mais quatro achados:

- Achado XX - Ausência de processo formal de trabalho para contratações de TI;
- Achado XXI - Ausência de análise de custo/benefício da solução de TI contratada;
- Achado XXII - Ausência de explicitação dos benefícios nas contratações de TI;
- Achado XXIII - Não-exigência de demonstrativo de formação de preço antes da adjudicação.

Critérios utilizados para o vigésimo achado:

a) Cobit 4.1 AI5.1 Procurement Control (Controle sobre aquisições – Desenvolver e seguir um conjunto de procedimentos e padrões consistente com o processo de licitação e a estratégia de aquisição gerais da organização para adquirir infraestrutura, instalações, hardware, software e serviços de TI necessários ao negócio).

Efeitos potenciais deste achado:

a) Aquisições de TI não alinhadas às necessidades de médio e longo prazos da organização;
b) Contratação de bens e serviços de TI que não atendem à qualidade necessária ao bom desenvolvimento do negócio do órgão/entidade;
c) Descumprimento de leis e normas relativas às licitações de TI;
d) Problemas na gestão dos contratos decorrentes de aquisições de TI por falta de requisitos previamente estabelecidos na licitação;
e) Desperdício de recursos.

Critérios utilizados para o vigésimo primeiro achado:

a) Cobit 4.1 AI1.3 Feasibility Study and Formulation of Alternative Courses of Action (Estudo de viabilidade e formulação de soluções alternativas – Desenvolver um estudo de viabilidade que examine a possibilidade da implementação dos requisitos. A gerência do negócio, apoiada pela gerência de TI, deve avaliar a viabilidade e as soluções alternativas e fazer uma recomendação ao patrocinador da ação);
b) Cobit 4.1 AI1.4 Requirements and Feasibility Decision and Approval (Decisão e aprovação dos requisitos e da viabilidade – Verificar se o processo requer que o patrocinador da ação formalize sua aprovação dos requisitos funcionais e técnicos e dos relatórios de estudo de viabilidade em etapas chave predeterminadas. O patrocinador da ação deve tomar a decisão final no que diz respeito à escolha da solução e da forma de sua aquisição).

Efeitos potenciais deste achado:

a) Contratação de bens e serviços de TI com custos acima do necessário;
b) Soluções alternativas satisfatórias e a um custo mais baixo não identificadas;
c) Desperdício de recursos.

Critérios utilizados para o vigésimo segundo achado:

a) Cobit 4.1 AI1.3 Feasibility Study and Formulation of Alternative Courses of Action (Estudo de viabilidade e formulação de soluções alternativas – Desenvolver um estudo de viabilidade que examine a possibilidade da implementação dos requisitos. A gerência do negócio, apoiada pela gerência de TI, deve avaliar a viabilidade e as soluções alternativas e fazer uma recomendação ao patrocinador da ação);
b) Cobit 4.1 AI1.4 Requirements and Feasibility Decision and Approval (Decisão e aprovação dos requisitos e da viabilidade – Verificar se o processo requer que o patrocinador da ação formalize sua aprovação dos requisitos funcionais e técnicos e dos relatórios de estudo de viabilidade em etapas chave predeterminadas. O patrocinador da ação deve tomar a decisão final no que diz respeito à escolha da solução e da forma de sua aquisição);
c) Acórdão 1.558/2003-TCU-Plenário, item 9.3.11;
d) Acórdão 2.094/2004-TCU-Plenário, item 9.1.1.

Efeitos potenciais deste achado:

a) Aquisições de TI não alinhadas às necessidades de médio e longo prazo da organização;
b) Contratação de bens e serviços de TI com desempenho abaixo do esperado e/ou requerido;
c) Contratação de bens e serviços de TI não integrados à infraestrutura de TI existente;
d) Desperdício de recursos.

Critérios utilizados para o vigésimo terceiro achado:

a) Lei n.º 8.666/1993, art. 7º, § 2º, inciso II, e art. 46, § 1º, inciso II.

Efeitos potenciais deste achado:

a) Problemas na gestão dos contratos decorrentes de aquisições de TI por falta de parâmetros para renegociação de valores, caso seja necessário;
b) Dificuldade de se identificar a prática de 'jogo de planilhas'

3.1.7. Processo de gestão de contratos de TI

O levantamento de informações constatou que 55% dos órgãos/entidades participantes do levantamento afirmou que não adota processo formal de trabalho para gestão de contratos de TI.

De acordo com o TCU, "a ausência desse processo de trabalho pode causar problemas ao bom funcionamento da área de TI da organização. Se os contratos de TI, que garantem os serviços de infraestrutura de TI, o desenvolvimento de aplicativos e o atendimento aos usuários, por exemplo, não forem bem geridos, todas as atividades de TI serão afetadas. Além disso, todas as atividades da organização que dependem de serviços de TI poderão sofrer com interrupções ou níveis de serviço abaixo do desejado e comprometer metas e objetivos da instituição."

Percebeu-se também que 65% dos órgãos/entidades que participaram do levantamento não realizavam reuniões periódicas com os contratados para avaliar o desempenho de cada contrato de TI. Além disso, 47% das organizações pesquisadas não definem previamente um critério para avaliação se as faturas apresentadas correspondem à realidade e se não contêm erros.

Segundo o Tribunal, "no levantamento, 90% das organizações consultadas disseram que fazem o monitoramento técnico dos contratos de TI. Foram informadas, também, a quantidade de contratos de TI e a quantidade de profissionais que executam essa tarefa. Em 17% dos órgãos/entidades pesquisados cada profissional monitora tecnicamente, em média, mais de cinco contratos de TI. A maior quantidade calculada foi de 14,7 contratos por pessoa e a menor foi de 0,5 contrato por pessoa. Deve-se ter sempre em mente que essas informações devem ser analisadas com cuidado porque esses contratos podem variar do fornecimento de um único item simples de ser controlado ao complexo controle de uma fábrica de software".

Das organizações consultadas, em menos da metade (45%) a monitoração administrativa é realizada por setor especializado não vinculado à área de TI. Nos outros 55%, uma parte significativa do tempo de profissionais especializados de TI é gasto no desempenho dessa tarefa.

Por fim, de acordo com o Tribunal, menos da metade (43%) dos órgãos/entidades participantes do levantamento informou que exige a transferência de conhecimento nos contratos relativos aos produtos e serviços de TI terceirizados. O percentual restante, 57%, é significativo, ainda mais quando são analisados alguns dos motivos que levam as organizações a terceirizarem serviços de TI: necessidade de acesso a tecnologias mais avançadas e redução de riscos associados a essas tecnologias.

O TCU afirma que "é um contrassenso a contratação de serviços importantes para a organização, mas para os quais não há os recursos necessários para serem realizados internamente, ou serviços que usem novas tecnologias e não ser exigida a transferência do conhecimento para sua realização. Deve-se observar que a organização paga inclusive pela aquisição do conhecimento por parte do prestador e, em muitos contratos, não assegura, ao seu término, a manutenção do conhecimento na instituição".

Dessa forma, o Tribunal elaborou mais cinco achados:

- Achado XXIV - Ausência de processo formal de trabalho para gestão de contratos de TI;
- Achado XXV - Não-realização de reuniões periódicas para avaliar o andamento dos contratos de TI;

- Achado XXVI - Não-definição prévia de itens para atestação técnica das faturas de contratos de TI;
- Achado XXVII - Monitoração administrativa dos contratos de TI feita pela área de TI;
- Achado XXVIII - Não-transferência de conhecimento relativo aos produtos e serviços terceirizados para os servidores dos órgãos/entidades.

Critérios para o vigésimo quarto achado:

a) Lei n.º 8.666/1993, Capítulo III – Dos Contratos;
b) Cobit 4.1 AI5.1 Procurement Control (Controle sobre aquisições – Desenvolver e seguir um conjunto de procedimentos e padrões consistente com o processo de licitação e a estratégia de aquisição gerais da organização para adquirir infraestrutura, instalações, hardware, software e serviços de TI necessários ao negócio).

Efeitos potenciais deste achado:

a) Descumprimento de leis e normas relativas à gestão de contratos de TI;
b) Problemas na gestão dos contratos de TI;
c) Baixa qualidade dos serviços prestados;
d) Não-aplicação de multas previstas nos contratos;
e) Interrupções na execução de contratos de TI;
f) Interrupção de processos que sustentam o negócio da organização;
g) Não-conclusão de projetos importantes para se atingir as metas da organização;
h) Desperdício de recursos.

Critérios para o vigésimo quinto achado:

a) Art. 67 da Lei n.º 8.666/1993;
b) Cobit 4.1 AI5.2 Supplier Contract Management (Gerenciamento de Contratos de Fornecedores – Definir um procedimento para estabelecimento, modificação e conclusão de contratos com todos os fornecedores. O procedimento deve cobrir, no mínimo, responsabilidades, obrigações e penalidades legais, financeiras, organizacionais, documentais, de desempenho, de segurança, de propriedade intelectual e de conclusão. Todos os contratos e aditivos devem ser revisados por consultores jurídicos);

c) Cobit 4.1 DS2.2 Supplier Relationship Management (Gerenciamento de Relacionamento com Fornecedores – Formalizar o processo de gerenciamento e relacionamento com cada fornecedor. O contato com o fornecedor deve tratar dos assuntos relativos a clientes e fornecedores e garantir a qualidade do relacionamento baseado na confiança e transparência, isto é, por meio de acordos de nível de serviço (SLA));
d) Cobit 4.1 DS2.3 Supplier Risk Management (Gerenciamento de Riscos com Fornecedores – Identificar e mitigar riscos relacionados à capacidade dos fornecedores de continuarem efetivamente a entregar os produtos de uma maneira segura, eficiente e contínua. Garantir que os contratos estejam de acordo com os padrões gerais do negócio e requisitos legais e regulatórios. O gerenciamento de riscos deve considerar antecipadamente acordos de não-divulgação de informações, contratos de garantia, viabilidade de continuidade do fornecedor, conformidade com requisitos de segurança, fornecedores alternativos, penalidades, recompensas etc.);
e) Cobit 4.1 DS2.4 Supplier Performance Monitoring (Monitoramento de Desempenho de Fornecedores – Estabelecer um processo para monitorar a entrega dos serviços de forma a garantir que o fornecedor esteja cumprindo os requisitos do negócio e continue seguindo os termos acordados no contrato e no SLA. Esse processo deve garantir, também, que o desempenho do fornecedor seja compatível com o de fornecedores alternativos e com as condições do mercado).

Efeitos potenciais deste achado:

a) Descumprimento de leis e normas relativas à gestão de contratos de TI;
b) Problemas na gestão dos contratos de TI;
c) Baixa qualidade dos serviços prestados;
d) Não-aplicação de multas previstas nos contratos;
e) Interrupções na execução de contratos de TI;
f) Interrupção de processos que sustentam o negócio da organização;
g) Não-conclusão de projetos importantes para se atingir as metas da organização;
h) Desperdício de recursos.

Critérios para o vigésimo sexto achado:

a) Cobit 4.1 DS2.4 Supplier Performance Monitoring (Monitoramento de Desempenho de Fornecedores – Estabelecer um processo para monitorar a entrega dos serviços de forma a garantir que o fornecedor esteja cumprindo os requisitos do negócio e

continue seguindo os termos acordados no contrato e no SLA. Esse processo deve garantir, também, que o desempenho do fornecedor seja compatível com o de fornecedores alternativos e com as condições do mercado).

Efeitos potenciais deste achado:

a) Descumprimento de leis e normas relativas à gestão de contratos de TI;
b) Pagamentos indevidos;
c) Não-aplicação de multas previstas nos contratos;
d) Desperdício de recursos.

Critérios para o vigésimo sétimo achado:

a) Art. 29 e inciso XIII do art. 55 da Lei n.º 8.666/1993;
b) Cobit 4.1 DS2.2 Supplier Relationship Management (Gerenciamento de Relacionamento com Fornecedores – Formalizar o processo de gerenciamento e relacionamento com cada fornecedor. O contato com o fornecedor deve tratar dos assuntos relativos a clientes e fornecedores e garantir a qualidade do relacionamento baseado na confiança e transparência, isto é, por meio de SLA).

Efeitos potenciais deste achado;

a) Descumprimento de leis e normas relativas à gestão de contratos de TI;
b) Pendências judiciais relativas a encargos trabalhistas e previdenciários;
c) Não-aplicação de multas previstas nos contratos.

Critérios para o vigésimo oitavo achado:

a) Cobit 4.1 AI4.4 Knowledge Transfer to Operations and Support Staff (Transferência de Conhecimentos para Equipes de Operação e Suporte – Transferir conhecimento e habilidades para permitir que equipes de operação e suporte técnico possam executar, dar suporte e manter efetiva e eficientemente o sistema e a infraestrutura associada).

Efeitos potenciais deste achado:

a) Problemas com a continuidade do serviço de TI após o fim do contrato;

b) Documentação insuficiente dos produtos advindos do contrato;
c) Serviço de ajuda (help-desk) sobrecarregado;
d) Perda de conhecimento importante para a organização;
e) Desperdício de recursos.

3.1.8. Processo orçamentário de TI

Apesar da maioria (61%) dos órgãos/entidades participantes do levantamento informar que, em 2006, foram levadas em consideração as ações previstas para o exercício seguinte na solicitação do orçamento para 2007, um percentual significativo (39%) não utilizou essas informações.

O Tribunal afirmou que "a partir desses dados, pode-se supor que 39% das organizações consultadas, quando da solicitação de orçamento para a área de TI em 2007, ou repetiram os valores do ano anterior ou simplesmente aplicaram um percentual de aumento linear sobre as despesas realizadas ou, ainda, acrescentaram um valor ao total do ano anterior sem a utilização de um critério transparente. Diante disso, verifica-se que a elaboração do orçamento para a área de TI nem sempre utiliza os insumos necessários à obtenção de resultado mais próximo da realidade".

Apesar de 82% dos órgãos/entidades consultados afirmarem que controlam os gastos de TI, um percentual considerável (21%) não enviou informações sobre o total de gastos com TI e uma parcela significativa, mesmo enviando os dados, informou que teve dificuldade em obter esses valores.

Além disso, pouco menos da metade (49%) das organizações consultadas disse que no 1º trimestre de 2007 fez a alocação orçamentária às ações constantes do planejamento de TI. Esse quadro, segundo o TCU, é um indício de que 51% dos pesquisados não exerce o controle sobre os gastos de TI a partir do orçamento aprovado e das ações planejadas. Provavelmente, essas organizações apenas atendem o que a legislação determina e não realizam um controle eficiente sobre os gastos de TI.

Dessa forma, são novos achados:

- Achado XXIX - Não-consideração das ações planejadas para o próximo ano quando da solicitação de orçamento para a área de TI;

- Achado XXX - Não-alocação dos recursos previstos no orçamento às ações constantes do planejamento de TI no início do ano

Critérios para o vigésimo nono achado:

a) Cobit 4.1 PO5.3 IT Budgeting (Orçamento de TI – Estabelecer e implementar práticas para elaborar um orçamento que reflita as prioridades estabelecidas na lista de projetos de TI e inclua os custos atuais de operação e manutenção da infraestrutura existente. As práticas devem dar suporte ao desenvolvimento de um orçamento geral para TI, assim como o desenvolvimento de orçamentos específicos para os projetos com ênfase específica nos componentes de TI. As práticas devem permitir revisão do andamento, refinamento das informações e aprovação do orçamento geral para TI e dos orçamentos específicos dos projetos).

Efeitos potenciais deste achado;

a) Recursos insuficientes para a área de TI;
b) Interrupção de serviços de TI por falta de recursos necessários;
c) Não-alcance de metas estabelecidas para a organização por falta de suporte da área de TI.

Critérios para o trigésimo achado:

a) Cobit 4.1 PO5.3 IT Budgeting (Orçamento de TI – Estabelecer e implementar práticas para elaborar um orçamento que reflita as prioridades estabelecidas na lista de projetos de TI e inclua os custos atuais de operação e manutenção da infraestrutura existente. As práticas devem dar suporte ao desenvolvimento de um orçamento geral para TI, assim como o desenvolvimento de orçamentos específicos para os projetos com ênfase específica nos componentes de TI. As práticas devem permitir revisão do andamento, refinamento das informações e aprovação do orçamento geral para TI e dos orçamentos específicos dos projetos).

Efeitos potenciais deste achado:

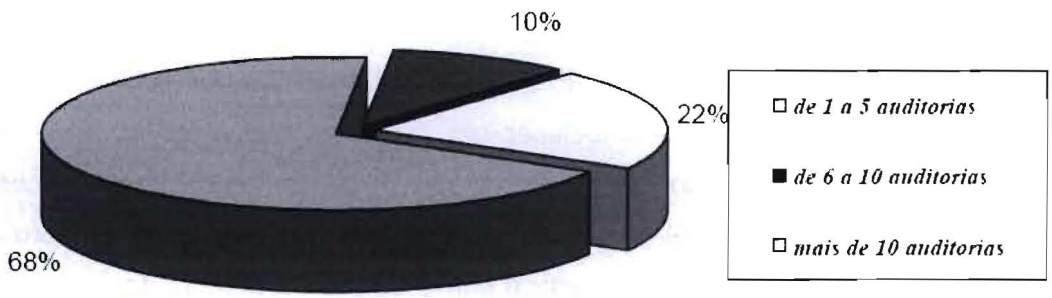
a) Recursos insuficientes para a área de TI;
b) Interrupção de serviços de TI por falta de recursos necessários;

c) Não-alcance de metas estabelecidas para a organização por falta de suporte da área de TI.

3.1.9. Auditoria de tecnologia da informação

Somente 40% dos pesquisados declarou ter realizado auditoria de TI nos últimos cinco anos no seu órgão/entidade. O Gráfico 5 estratifica a quantidade de auditorias de TI realizadas nessas 101 organizações.

Gráfico 5 - Quantidade de auditorias de TI realizadas nos últimos cinco anos



Fonte: Acórdão n.º 1.603/2008 - Tribunal de Contas da União

De acordo com o TCU, "a auditoria de TI consiste em verificar um ou vários aspectos da governança de TI de uma organização. Note-se que essa ainda é uma definição ampla e abrange vários tipos e perspectivas para auditorias. Assim, uma auditoria de TI pode, por exemplo, avaliar apenas controles de acesso lógico ao ambiente de TI, por meio de análise de vulnerabilidade. Já se for realizada com um objetivo mais gerencial, a auditoria pode avaliar se os processos de TI ligados ao desenvolvimento de sistemas, por exemplo, estão sendo executados conforme a política da empresa e estão gerando sistemas eficazes. Outra possibilidade é uma auditoria para verificar a integridade e fidedignidade das informações armazenadas nas bases de dados da organização. Ou, ainda, pode-se verificar se a contratação de bens e serviços de TI é feita de acordo com as normas da organização e a legislação vigente".

Apenas 19% dos pesquisados declararam ter equipe interna para auditoria de TI. Dessa forma, para muitos, a auditoria de TI somente é realizada por auditores/consultores independentes ou por organizações reguladoras, como o TCU e CGU.

Observa-se, também, que dentre as auditorias realizadas, a maior quantidade delas (32%) está focada na aquisição de bens e serviços de TI, seguida das auditorias com foco em segurança da informação (20%). Uma possível explicação é que as organizações que executam tais auditorias o fazem em função de exigências legais de agências reguladoras, mais do que por necessidades de gestão.

Assim, foram elaborados os dois últimos achados:

- Achado XXXI - Inexecução de auditoria de TI pelos órgãos/entidades;
- Achado XXXII - Inexistência de equipe própria para realizar auditoria de TI.

Critérios para o trigésimo primeiro achado:

a) Cobit 4.1 ME2 Monitor and Evaluate Internal Control (Monitorar e Avaliar os Controles Internos – Estabelecer um programa efetivo de controle interno de TI requer um processo bem definido de monitoramento. Esse processo inclui o monitoramento e o relato das exceções de controle, resultados de auto avaliações e revisão de terceiros. Um benefício chave do monitoramento dos controles internos é prover segurança com vistas a operações efetivas e eficientes e conformidade com leis e regulações);
b) NBR ISO/IEC 17799:2005, item 15.2 – Conformidade com normas e políticas de segurança da informação e conformidade técnica: convém que a segurança dos sistemas de informação seja analisada criticamente a intervalos regulares;
c) NBR ISO/IEC 17799:2005, item 6.1.8 – Análise crítica independente de segurança da informação: convém que o enfoque da organização para gerenciar a segurança da informação e a sua implementação (...) seja analisado criticamente, de forma independente, a intervalos planejados, ou quando ocorrerem mudanças significativas relativas à implementação da segurança da informação.

Efeitos potenciais para este achado:

a) Inobservância da política de segurança da informação da organização quando da implementação dos controles de acesso lógico nos sistemas de informação;
b) Existência de informações não confiáveis na base de dados da organização, o que compromete não só a efetividade dos seus sistemas de informação como a de sistemas de outras organizações que utilizam essa mesma base de dados;

c) Área de TI com governança imatura, sem controles e indicadores que possam apontar os problemas e oportunidades de negócio para a organização.

Critérios para o trigésimo segundo achado:

a) Cobit 4.1 ME2 Monitor and Evaluate Internal Control (Monitorar e Avaliar os Controles Internos – Estabelecer um programa efetivo de controle interno de TI requer um processo bem definido de monitoramento. Esse processo inclui o monitoramento e o relato das exceções de controle, resultados de auto avaliações e revisão de terceiros. Um benefício chave do monitoramento dos controles internos é prover segurança com vistas a operações efetivas e eficientes e conformidade com leis e regulações);
b) NBR ISO/IEC 17799:2005, item 15.2 – Conformidade com normas e políticas de segurança da informação e conformidade técnica: convém que a segurança dos sistemas de informação seja analisada criticamente a intervalos regulares.

Efeitos potenciais deste achado:

a) Ausência de auditores internos que poderiam auxiliar em auditorias de processos de gestão.

3.1.10. Conclusão

O TCU chegou à seguinte conclusão decorrente dos dados obtidos no levantamento de informação de governança de TI:

"Diante do quadro apresentado, observa-se que a situação da governança de TI na Administração Pública Federal é bastante heterogênea do ponto de vista dos seus diversos aspectos. Os aspectos que de alguma forma são regulados por leis e normas (processo orçamentário e contratação e gestão de bens e serviços de TI), somados a planejamento estratégico, desenvolvimento de sistemas, gestão de níveis de serviço e auditoria de TI, apresentam algum desenvolvimento, apesar de estarem longe do ideal. A questão de estrutura de pessoal de TI é bastante diversa e está atrelada à natureza jurídica da organização".

"O aspecto em que a situação da governança de TI está mais crítica é no que diz respeito ao tratamento da segurança da informação. Conclui-se que essa é uma área em que o TCU pode e deve atuar como indutor do processo de aperfeiçoamento da governança de TI. O Tribunal já acertou, inclusive, ao editar, em 2003 e 2007, a 'Cartilha de Segurança da Informação' para servir como orientação sobre o tema. Outra maneira de induzir a melhoria no tratamento da segurança é a realização de auditorias de TI com foco em segurança da informação, que poderão fornecer subsídios valiosos para os gestores sobre os principais controles que devem ser implementados visando garantir a confiabilidade, a integridade e a disponibilidade das informações tratadas pelos órgãos/entidades da Administração Pública Federal".

3.2. Levantamento de Informações de 2010

A Secretaria de Fiscalização de Tecnologia da Informação - SEFTI, do Tribunal de Contas da União, em cumprimento à determinação formulada pelo acórdão 1.603/2008 - Plenário, realizou levantamento destinado a verificar a evolução da governança de TI em relação à situação encontrada em 2007, no âmbito da Administração Pública Federal.

Durante a fase de planejamento, foram elaboradas 30 questões, subdivididas em 152 itens, organizadas segundo sete (das oito) dimensões do Gespública: liderança, estratégias e planos, cidadãos, sociedade, informações e conhecimento, pessoas e processos.

Cabe esclarecer que o Gespública é um programa federal estabelecido pelo Decreto nº 5.378, de 23 de fevereiro de 2005, e coordenado pelo Ministério do Planejamento, Orçamento e Gestão. Esse programa é voltado para orientar e aferir a qualidade da gestão pública.

Além do Gespública, foram utilizados como critérios o Cobit 4.1 (Control Objectives for Information and related Technology) (ITGI, 2007), a ABNT NBR ISO/IEC 27002 – segurança da informação (ABNT, 2005) e a ABNT NBR ISO/IEC 38500 – governança corporativa de TI (ABNT, 2009).

No levantamento, foram selecionadas 315 instituições da Administração Pública Federal. Até o fechamento do relatório, 265 instituições haviam atendido à solicitação de

remessa de informações, enquanto 50 instituições não responderam o questionário até o encerramento deste relatório.

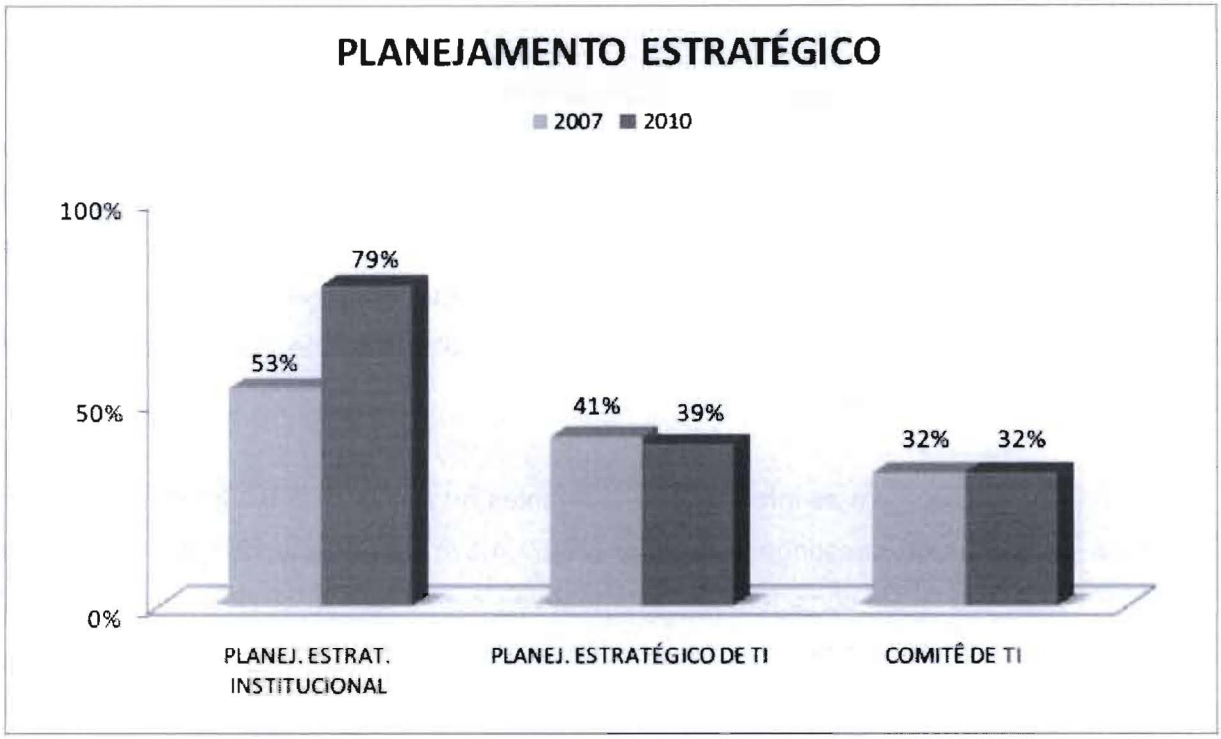
Com vistas a facilitar a análise das informações, os respondentes foram divididos em segmentos: EXE-Dest: abrange as empresas públicas federais e as sociedades de economia mista; EXE-Sisp: abrange as instituições que fazem parte do Sistema de Administração dos Recursos de Informação e Informática (Sisp); JUD: abrange as instituições que fazem parte do Poder Judiciário; LEG: abrange as instituições que fazem parte do Poder Legislativo; e MPU: abrange as instituições que fazem parte do Ministério Público da União (MPU).

De acordo com as informações constantes no relatório do levantamento, das trinta e nove perguntas do questionário anterior (2007), nove foram excluídas do levantamento de 2010, visto que foram consideradas incompatíveis com o foco dado no levantamento. Outras perguntas não encontraram correspondência direta, visto que o questionário de 2010 enfatizou a maturidade dos processos de trabalho, no lugar da anterior ênfase em artefatos ou detalhes de procedimentos.

3.2.1. Planejamento Estratégico Institucional e de TI

De acordo com os dados obtidos, o número de entes que fazem planejamento estratégico institucional aumentou, ao passo que há certa estabilidade no número de instituições que fazem planejamento de TI e que têm comitê de TI.

Gráfico 6 - Evolução dos indicadores de Planejamento Estratégico



Fonte: Acórdão n.° 2.308/2010 - Tribunal de Contas da União

Essa evolução no indicador de planejamento estratégico institucional, de acordo com o TCU, deve-se, em grande parte, à resposta dos órgãos do judiciário à atuação do Conselho Nacional de Justiça (CNJ), por meio da Resolução nº 70/2009. Ressalte-se que também houve evolução relevante nos órgãos pertencente ao Sisp.

Segundo o Tribunal, "quanto ao planejamento de TI, causa preocupação a sua ausência em 61% das instituições públicas pesquisadas, pois a jurisprudência do TCU é pacífica quanto à necessidade de planejar as contratações de TI em harmonia com o planejamento estratégico institucional e com o plano diretor de tecnologia da informação – PDTI (são exemplos os acórdãos nº 1.521 e 1.558/2003, 2.094/2004, 786/2006 e 1.603/2008, todos do Plenário do TCU)".

Verifica-se que a ausência de PDTI sugere que há contratações de TI sendo empreendidas em desacordo com a legislação e jurisprudência.

3.2.2. Estrutura de Pessoal de TI

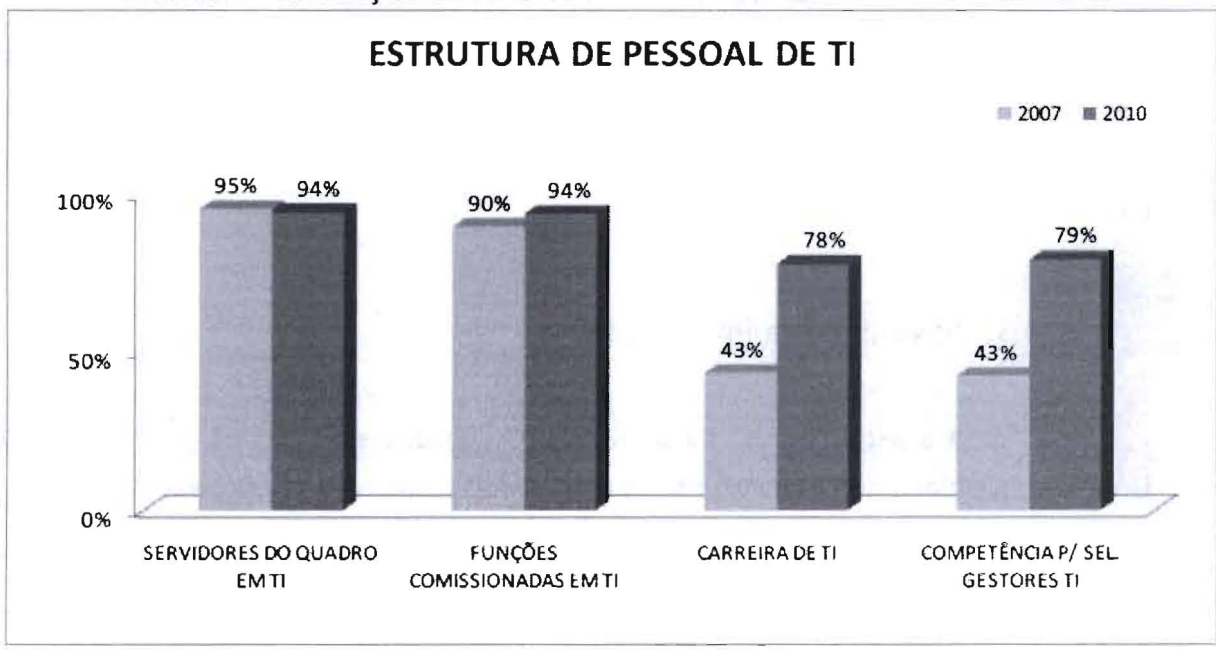
De acordo com os novos dados, 94% das instituições afirmaram ter servidores do próprio quadro atuando na área de TI, número bastante elevado e semelhante ao obtido em

2007. Porém, segundo o TCU, causa preocupação que em 6% das instituições a TI organizacional seja controlada por pessoas estranhas ao quadro interno, visto que os riscos de TI podem ser maiores nesses casos, como ressaltado pelo item 9.1.2 do Acórdão nº 1.603/2008-TCU-Plenário.

De modo semelhante, 94% das instituições respondentes têm funções comissionadas voltadas para a gestão de TI, número bastante elevado e que representa leve crescimento em relação a 2007. Entretanto, de acordo com o Tribunal, também causa preocupação que 6% das instituições respondentes ainda mantenham a gestão de TI sob o comando de servidores não comissionados ou de terceiros.

Quanto à existência de carreira de TI, o índice evoluiu de 43% para 78% e, com relação ao modo de seleção dos gestores de TI, de 2007 a 2010, o percentual das instituições que afirmaram selecionar seus gestores de TI por critérios de competência aumentou de 43% para 79%.

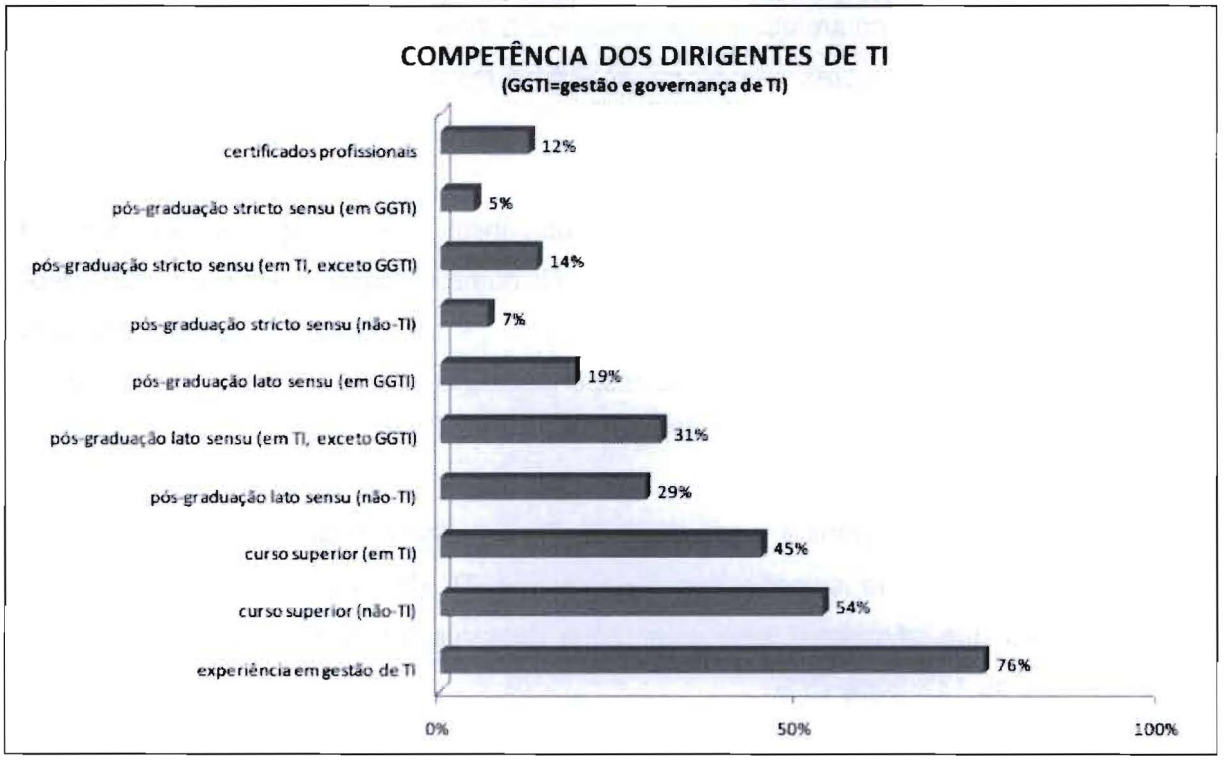
Gráfico 7 - Evolução dos indicadores de Estrutura de Pessoal de TI



Fonte: Acórdão n.º 2.308/2010 - Tribunal de Contas da União

O levantamento de 2010 também procurou detalhar o exame das competências dos dirigentes de TI, cujo resultado é apresentado na figura abaixo:

Gráfico 8 - Competências dos dirigentes de TI



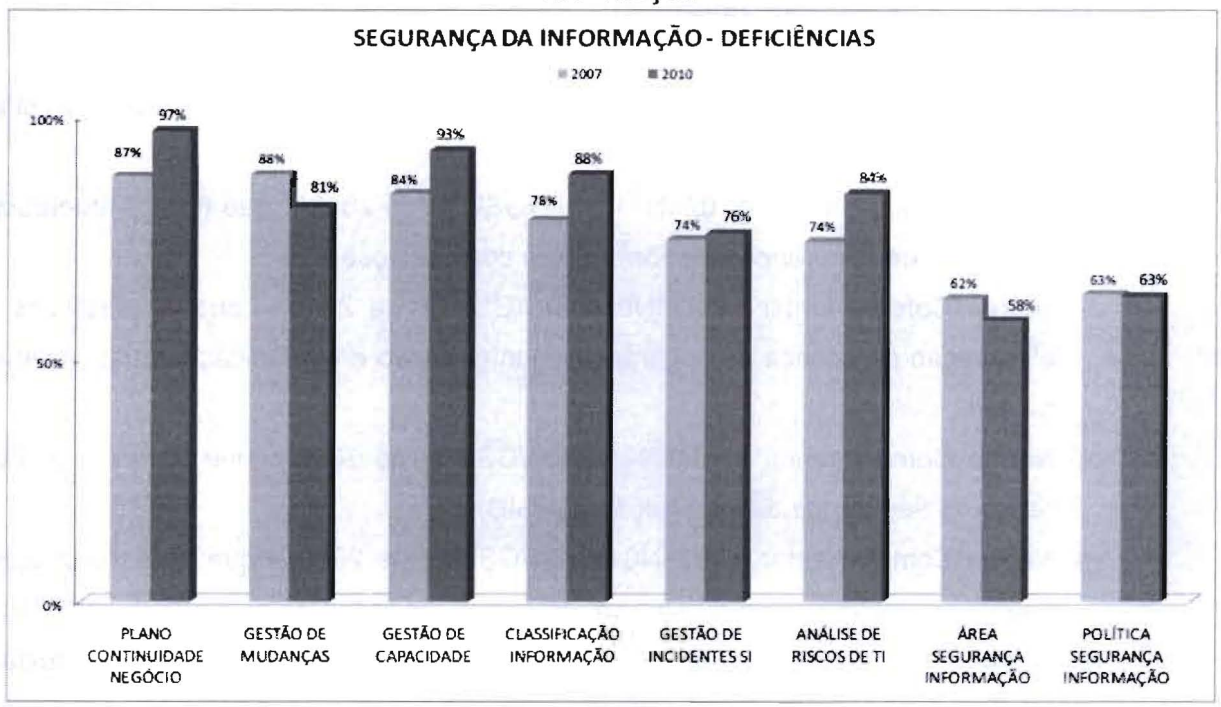
Fonte: Acórdão n.° 2.308/2010 - Tribunal de Contas da União

Segundo o TCU, "estes números reforçam a impressão de que ainda é muito baixo o investimento das instituições na preparação de gestores de TI para efetivamente gerenciar a TI institucional, especialmente em contextos de alto requerimento de governança corporativa e de TI".

3.2.3. Segurança da Informação

A figura a seguir apresenta os resultados obtidos em 2010 comparados em 2007. Deve ser salientado que o gráfico se refere à ausência das práticas recomendadas.

Gráfico 9 - Evolução dos indicadores de Deficiências em Segurança da Informação



Fonte: Acórdão n.º 2.308/2010 - Tribunal de Contas da União

De acordo com o Tribunal de Contas da União, "inicialmente, admite-se por prudência que a piora em parte dos indicadores pode não refletir uma efetiva deterioração da situação da segurança da informação na APF, mas uma possível melhora na compreensão, por parte dos respondentes, dos conceitos questionados. Infere-se que essa melhor compreensão tenha resultado em avaliações mais rigorosas no presente levantamento".

Percebe-se que, em todos os casos, não houve melhora nos processos que tratam de segurança da informação na APF. Ou seja, se em 2007 a situação já se mostrava preocupante, atualmente é ainda pior, uma vez que o alarme foi soado por meio do Acórdão nº 1.603/2008-TCU-Plenário e, um ano e meio depois, o quadro não apresenta evidências de melhora.

Segundo o TCU, "o mínimo esperado é que se empreenda uma análise de riscos (menos de 20% o fazem segundo os dados coletados) e que, a partir daí, se busque uma estratégia adequada à realidade de cada instituição. Mesmo que a decisão tomada a partir do conhecimento de determinado risco seja aceitá-lo, é necessário que esse risco seja conhecido e suas consequências estimadas".

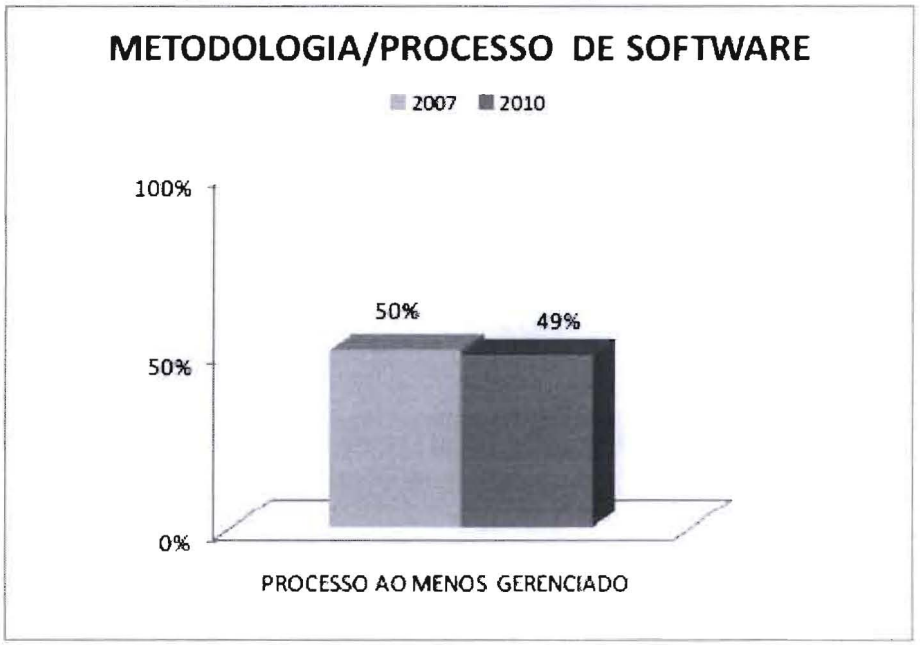
Por fim, deve-se mencionar que, sobre esse tema, o Gabinete de Segurança Institucional (GSI) publicou as seguintes normas:

a) Instrução Normativa GSI/PR nº 1, de 13 de junho de 2008 – que trata da Gestão de Segurança da Informação e Comunicações na APF;
b) Norma Complementar nº 02/IN01/DSIC/GSI/PR de 2008 – que trata da metodologia de gestão de segurança da informação e comunicações;
c) Norma Complementar nº 03/IN01/DSIC/GSI/PR de 2009 – que dá diretrizes para elaboração de política de segurança da informação e comunicações nas instituições da APF;
d) Norma Complementar nº 04/IN01/DSIC/GSI/PR de 2009 – que trata da gestão de riscos de segurança da informação (GRSIC);
e) Norma Complementar nº 05/IN01/DSIC/GSI/PR de 2009 – que trata da criação de equipes de tratamento e resposta a incidentes em redes de computadores (ETIR)
f) Norma Complementar nº 06/IN01/DSIC/GSI/PR de 2009 – que trata da gestão de continuidade de negócios em segurança da informação e comunicações;
g) Norma Complementar nº 07/IN01/DSIC/GSI/PR de 2010 – que trata de controles de acesso.

3.2.4. Desenvolvimento de Software

Segue a comparação dos resultados obtidos em 2007 para a pergunta "o desenvolvimento de sistemas segue alguma metodologia?" com os obtidos no levantamento de 2010. Cabe destacar que, segundo o TCU, "a nomenclatura 'metodologia' para tratar de desenvolvimento de sistemas, utilizada no levantamento de 2007, foi substituída por 'processo de software', em consonância com as normas técnicas vigentes, em especial a ABNT NBR ISO/IEC 15.504".

Gráfico 10 - Evolução dos indicadores de adoção de Processo de Software



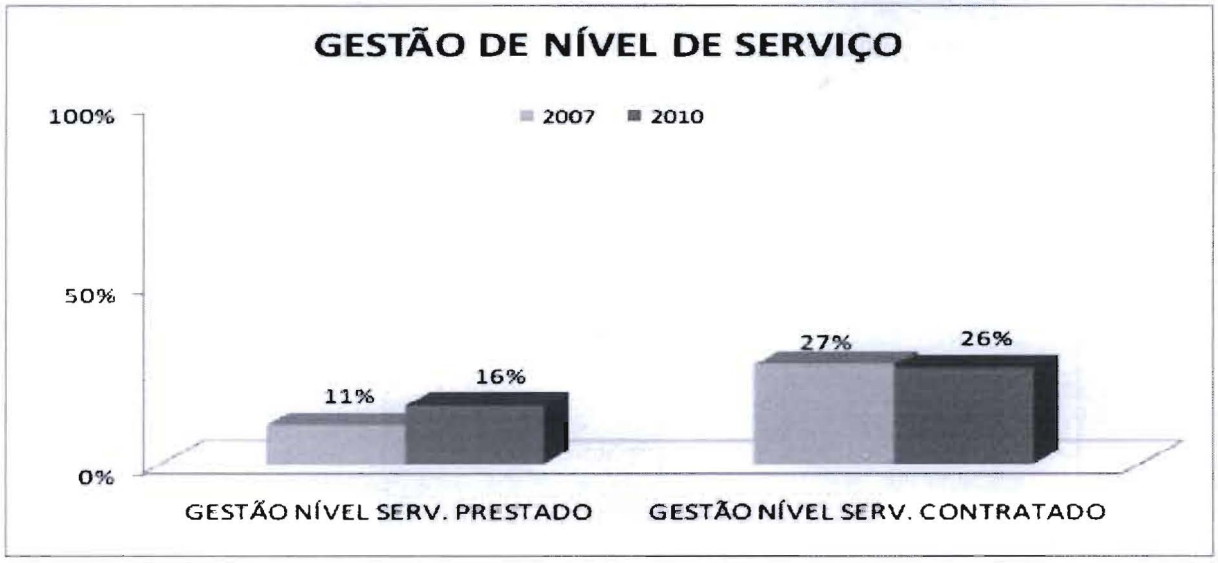
Fonte: Acórdão n.º 2.308/2010 - Tribunal de Contas da União

Com base nos dados analisados, o Tribunal de Contas da União constatou que "menos da metade das instituições possuem o instrumento que, se usado adequadamente pode não só disciplinar o desenvolvimento de software na instituição, como apoiar a aquisição de software e servir de parâmetro para aferir qualidade dos produtos recebidos".

3.2.5. Gestão de Níveis de Serviço

De acordo com as novas informações obtidas, em 2010, apenas 16% das instituições declararam se atentar à gestão do nível de serviços oferecido pela área de TI. Em relação à gestão do nível de serviço em contratação houve queda do percentual: de 27% em 2007, para 26% em 2010.

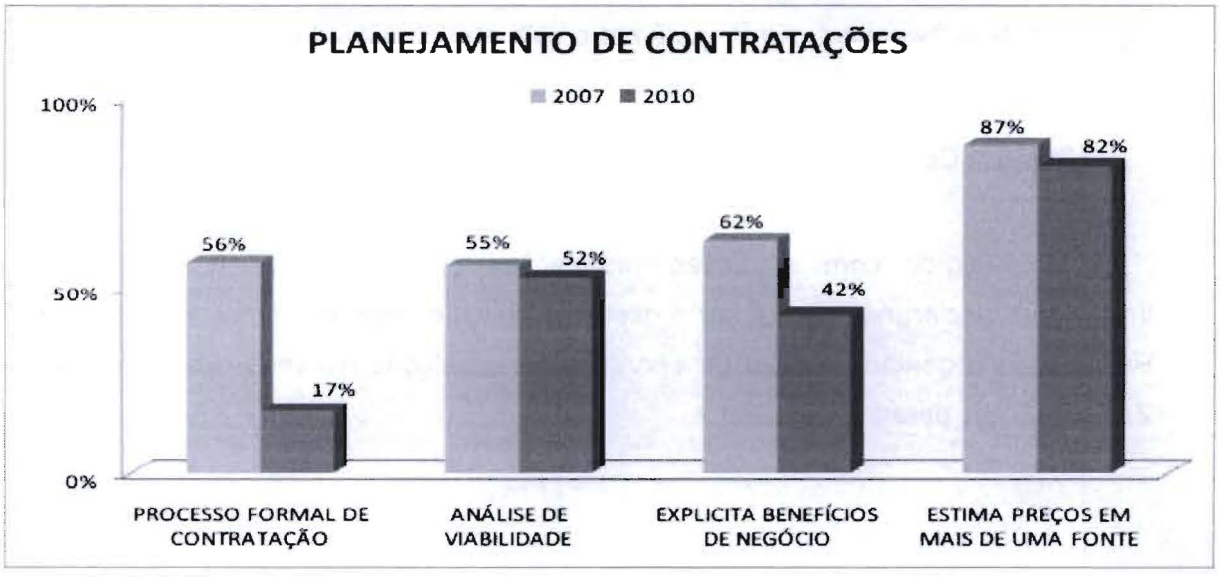
Gráfico 11 - Evolução dos indicadores de Gestão de Nível de Serviço



Fonte: Acórdão n.° 2.308/2010 - Tribunal de Contas da União

3.2.6. Processos de Contratação e Gestão de Contratos de TI

Gráfico 12 - Evolução dos indicadores de Planejamento de Contratações



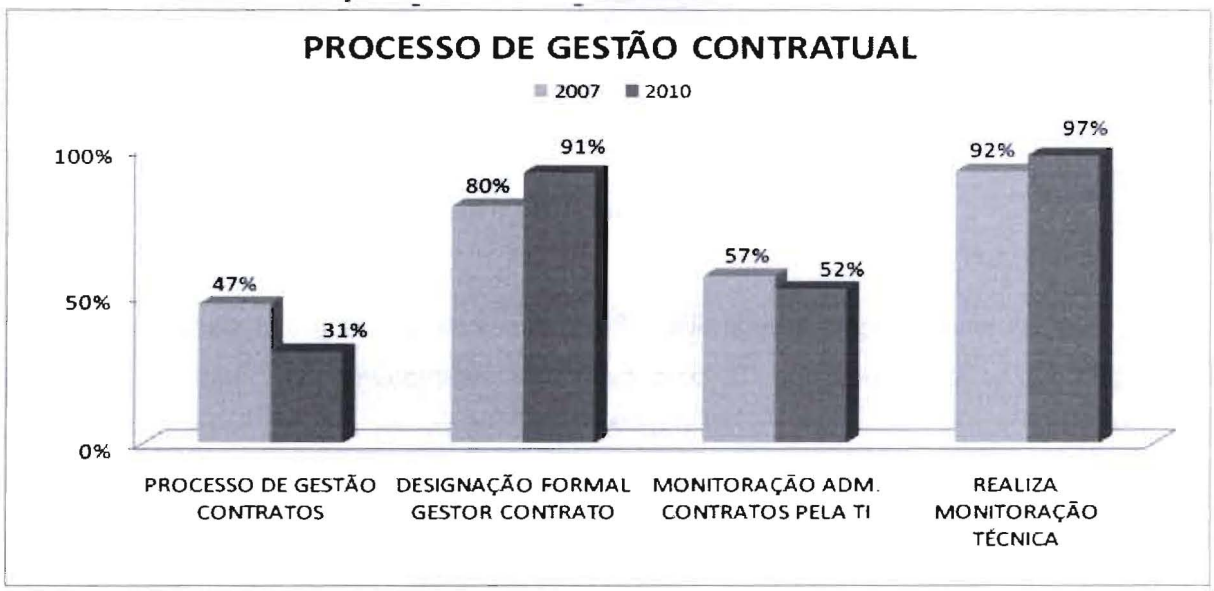
Fonte: Acórdão n.° 2.308/2010 - Tribunal de Contas da União

De acordo com o TCU, "a pergunta acerca do processo formal de contratação, em 2007, buscava obter informações acerca de instituições que haviam disciplinado os procedimentos a serem empreendidos até o momento da celebração do contrato. Entretanto, avalia-se que, naquele levantamento, essa questão não foi bem compreendida por diversas instituições, que responderam positivamente considerando normas gerais, como a própria Lei de Licitações, como sendo seu processo de trabalho".

Dessa forma, segundo o Tribunal, não se deve interpretar a deterioração acentuada no índice 'processo formal de contratação' como um retrocesso, mas tão somente como uma informação mais precisa acerca da falta de preparo da Administração para gerir suas contratações por meio de processos definidos e mensuráveis.

Por fim, o Tribunal constatou que as informações colhidas no trabalho em análise revelaram um quadro ainda mais crítico, no qual, quase como regra, a Administração não planeja suas contratações de TI seguindo processos de trabalho formais e definidos.

Gráfico 13 - Evolução dos indicadores de Processo de Gestão Contratual



Fonte: Acórdão n.° 2.308/2010 - Tribunal de Contas da União

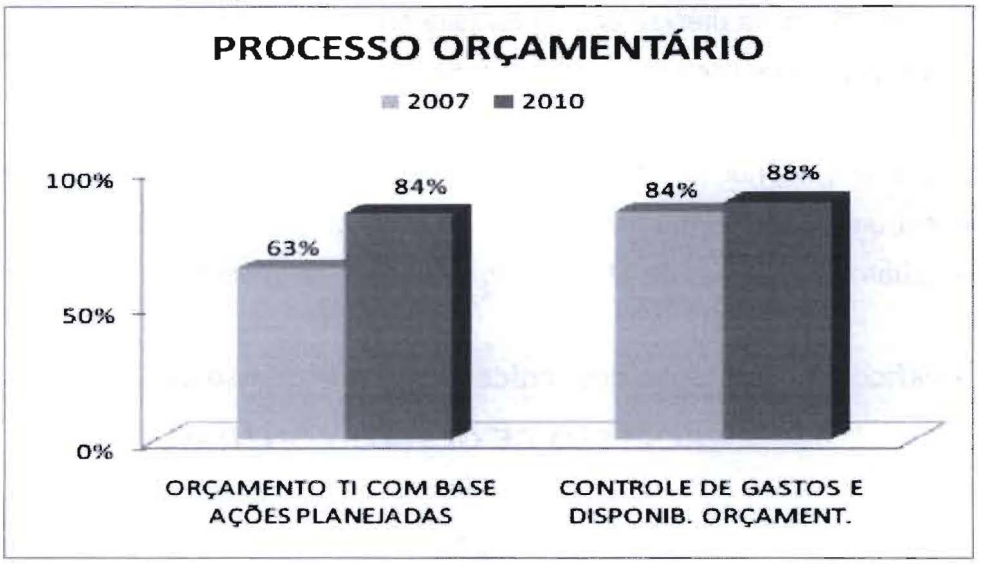
Com relação ao processo de gestão contratual, o Tribunal entendeu que, no levantamento realizado em 2007, a pergunta acerca do processo formal de gestão contratual também não foi bem compreendida por diversos respondentes.

Dessa forma, o TCU dispõe que não se deve interpretar a deterioração no índice "processo de gestão de contratos" como um retrocesso, mas como uma informação mais acurada acerca da falta de preparo da Administração para gerir seus contratos por meio de processos definidos e mensuráveis.

Verifica-se melhora em quesitos como designação formal de gestor de contrato e realização de monitoração técnica.

3.2.7. Processo Orçamentário de TI

Gráfico 14 - Evolução dos indicadores de Processo Orçamentário de TI

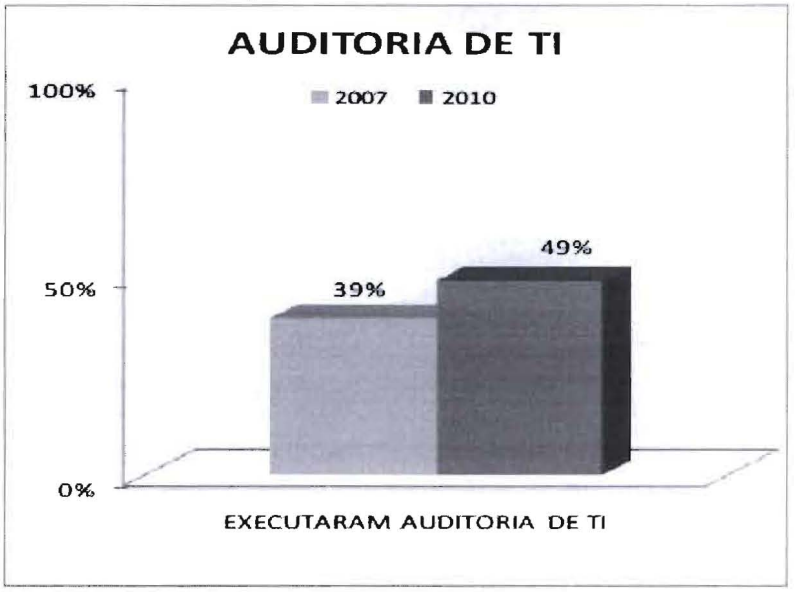


Fonte: Acórdão n.° 2.308/2010 - Tribunal de Contas da União

No levantamento em análise, 84% das instituições respondentes declararam ter elaborado o orçamento de TI com base nas estimativas de custos das contratações previstas. Além disso, 88% declararam controlar os gastos e a disponibilidade orçamentária de tecnologia da informação.

3.2.8. Auditoria de TI

Gráfico 15 - Evolução dos indicadores de Auditoria de TI

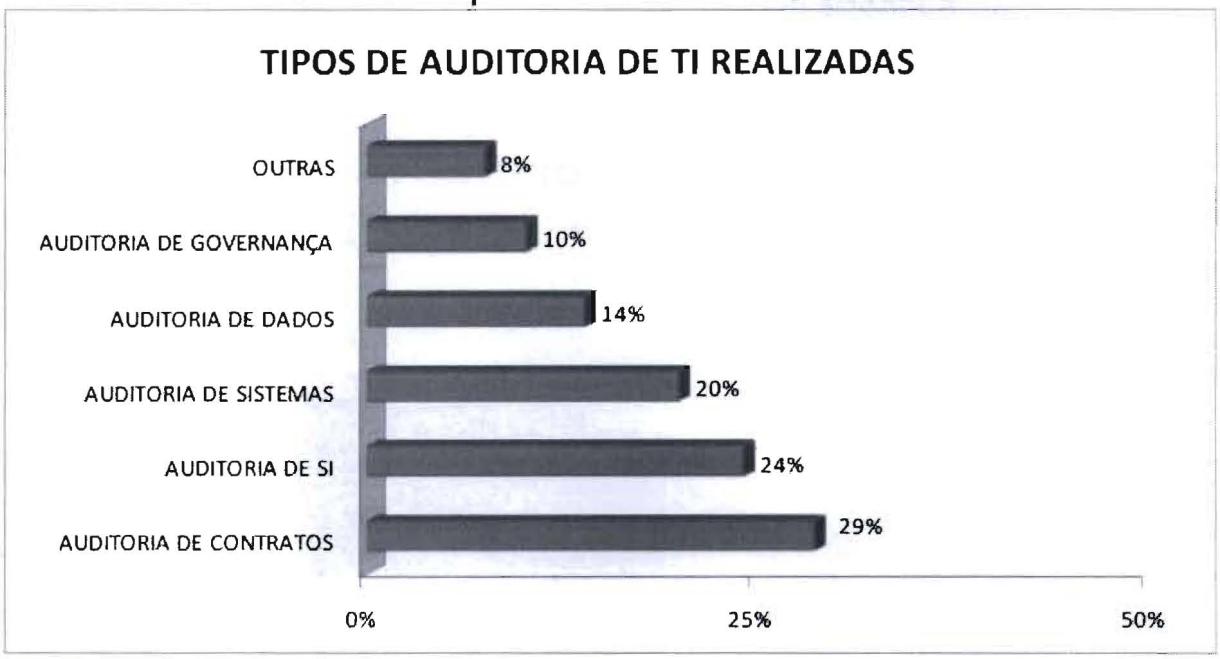


Fonte: Acórdão n.° 2.308/2010 - Tribunal de Contas da União

De acordo com o TCU, no presente levantamento, a pergunta se referiu à realização de auditoria de TI empreendida por iniciativa própria, caso em que é demonstrada a preocupação da instituição com o controle da sua TI. Além disso, tendo em vista que o intervalo desde o último levantamento foi de três anos, considerou-se esse horizonte no questionário.

A figura a seguir detalha os tipos de auditoria realizados:

Gráfico 16 - Tipos de Auditoria de TI realizadas



Fonte: Acórdão n.° 2.308/2010 - Tribunal de Contas da União

3.2.9. Liderança

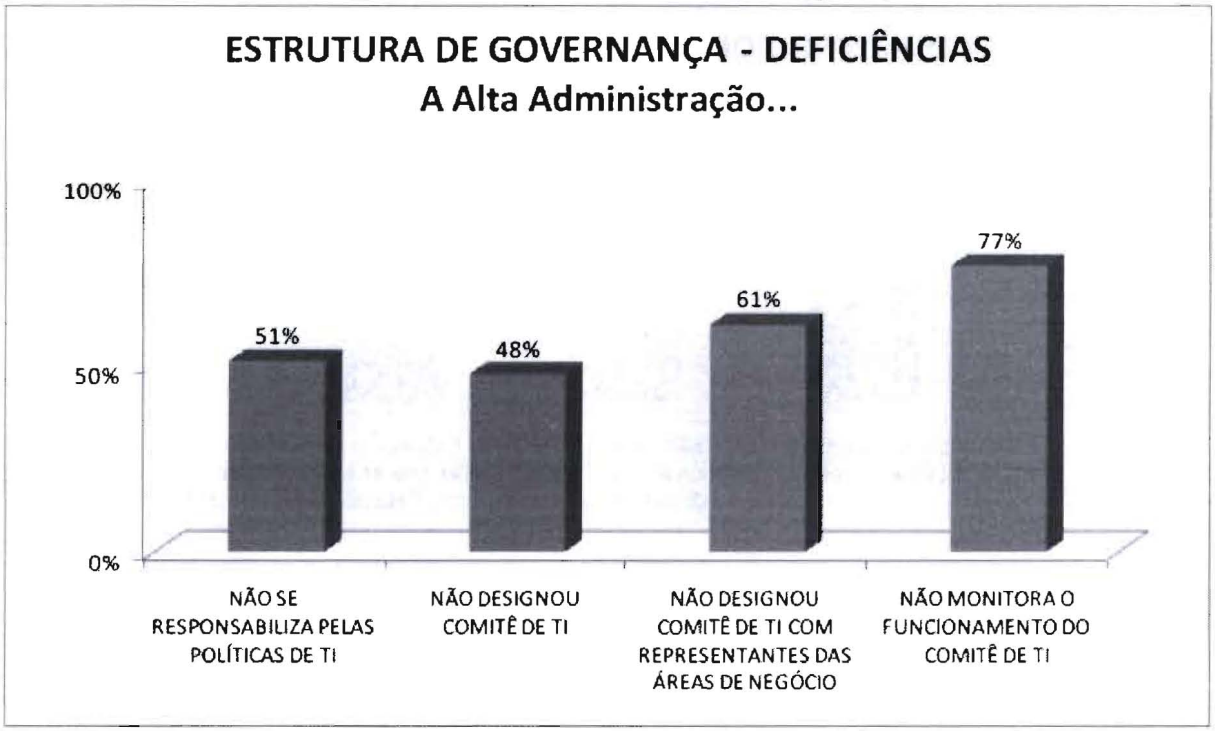
De acordo com afirmações constantes no próprio levantamento de informações, é da Alta Administração a responsabilidade de governar a TI, ou seja, de garantir que a TI funcione de forma integrada e que agregue valor ao negócio.

No entanto, segundo o TCU, há alguns elementos importantes que devem ser implantados para que esse governo seja efetivo, entre os quais se destaca a dimensão "Liderança", apresentada a seguir.

Registre-se que os próximos questionamentos não foram incluídos no levantamento de 2007, não possuindo, portanto, dados comparativos.

3.2.10. Estrutura de Governança de TI

Gráfico 17 - Estrutura de Governança de TI



Fonte: Acórdão n.° 2.308/2010 - Tribunal de Contas da União

Com base nos dados do gráfico acima, segundo o Tribunal de Contas da União, é possível supor que a maioria das instituições da APF ainda não se preocupa com governança de TI. Ainda de acordo com o Tribunal, "não há como se falar em governança de TI se a alta administração não estabelece ou responde pelas diretrizes mais elementares".

Segundo a Corte, "o baixo índice de comitês de TI instituídos e acompanhados pode ser explicado pela falta de consciência da alta administração acerca de seu papel na governança de TI: um dirigente que não se responsabiliza pelas políticas de TI, não sentirá necessidade do apoio de um comitê, menos ainda de acompanhar seu funcionamento".

3.2.11. Desempenho Institucional na Gestão e no Uso de TI

Gráfico 18 - Desempenho Institucional em Gestão de TI

Fonte: Acórdão n.° 2.308/2010 - Tribunal de Contas da União

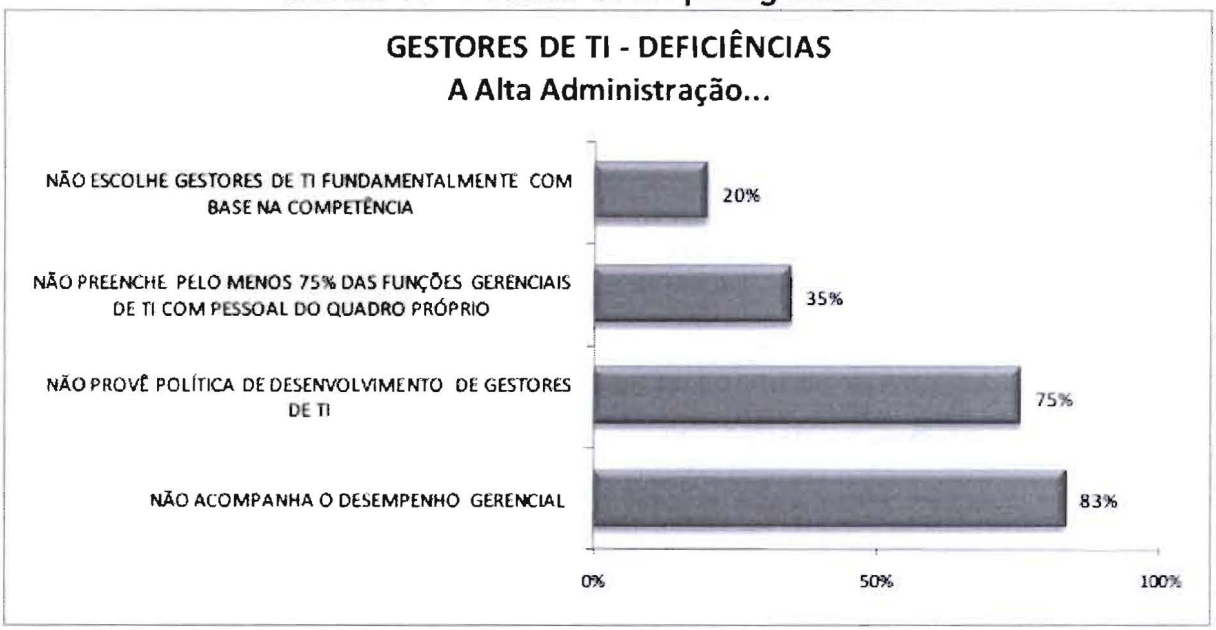
Segundo o TCU, "para que se possa acompanhar o desempenho da gestão e do uso da TI, é preciso primeiro definir parâmetros para isso. O primeiro passo é definir os objetivos. Em seguida, é importante definir indicadores de desempenho. Com eles, torna-se possível avaliar o grau de alcance dos objetivos previamente definidos. Por fim, para que esses indicadores sejam úteis, eles devem ser monitorados regularmente. Essa avaliação periódica dos indicadores de desempenho subsidia as decisões que permitem as correções necessárias para o alcance dos objetivos definidos inicialmente".

Os dados encontrados no levantamento indicaram que ao menos 57% dos respondentes não definiram objetivos de desempenho para o uso e para a gestão da TI institucional. Esse número, considerado muito alto, é ainda mais enfraquecido pelo fato de que ao menos 76% não estabelecem indicadores de desempenho para TI, 71% não avaliam regularmente esse desempenho e 87% admitiram não tomar suas decisões quanto ao uso e à gestão de TI com base nos benefícios esperados dos sistemas de informação.

Dessa forma, a maioria das instituições respondentes não estabelece objetivos de TI, não têm indicadores de desempenho para esses objetivos, não avalia o alcance de objetivos e não toma decisões com base nos benefícios de negócio advindos dos sistemas de informação providos pela TI.

3.2.12. Gestores de Tecnologia da Informação

Gráfico 19 - Política de RH para gestão de TI



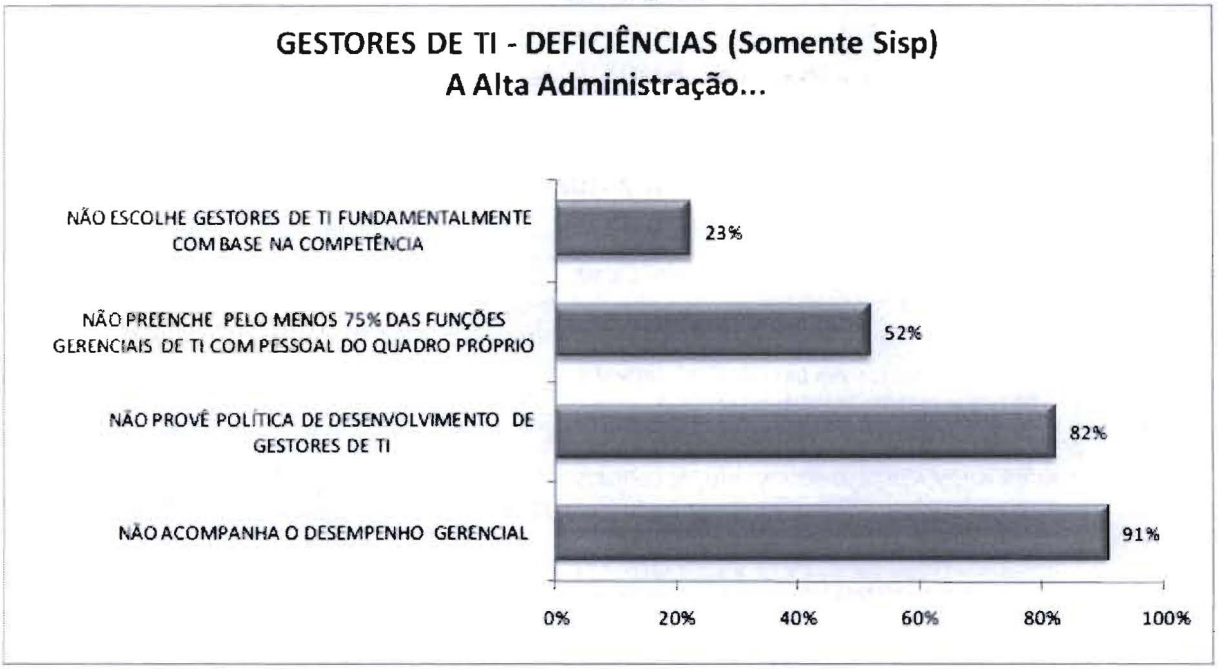
Fonte: Acórdão n.º 2.308/2010 - Tribunal de Contas da União

De acordo com o TCU, o foco desta questão no levantamento relaciona-se especificamente aos gestores inseridos na área de TI, cujas decisões devem balancear aspectos técnicos, administrativos e de negócio, contribuindo para a efetividade e a eficiência da instituição, em parceria com os demais decisores da instituição. Porém, conforme pode ser percebido pela análise do gráfico acima, os resultados foram alarmantes.

O Tribunal concluiu que "esses indicadores apontam para a falta de preocupação da alta administração em garantir uma boa capacidade gerencial interna".

A situação é especialmente delicada no caso do Sisp, onde pelo menos 52% dos respondentes não priorizam o preenchimento das funções de gestão de TI com pessoas do quadro interno, como pode ser visto na figura abaixo.

Gráfico 20 - Política de RH para gestão de TI (somente Sisp)



Fonte: Acórdão n.° 2.308/2010 - Tribunal de Contas da União

3.2.13. Conclusão

Segundo o Tribunal de Contas da União: "a adoção dos conceitos de governança de TI pela APF ainda é incipiente, pois a maioria das instituições respondentes encontra-se em estágio inicial. Os dados coletados não deixam margem à dúvida de que a situação da governança de TI na APF ainda se encontra em estado precário. Como a maioria das instituições respondentes encontra-se em estágio inicial (...), pode-se inferir que a adoção dos conceitos de governança de TI pela APF ainda é incipiente.

No que se refere aos instrumentos básicos para a alta administração governar a TI de forma minimamente efetiva (por exemplo, pela designação de um comitê de TI, pela definição de objetivos de desempenho e pelo monitoramento desse desempenho), o quadro também não é bom. Aparentemente, ainda é uma novidade o conceito de que governar a TI, por se tratar de uma área crítica para o alcance dos objetivos da instituição, é responsabilidade da alta administração. Causa espécie que aproximadamente metade dos respondentes tenha declarado que não se enxerga como responsável pelas políticas corporativas de TI. Ressalte-se que as respostas foram dadas, na grande maioria dos casos, pelo dirigente máximo da instituição.

Na comparação com o levantamento de 2007, é preocupante a falta de evolução perceptível na área de segurança da informação, que continua com índices de não conformidade muito altos. Além disso, o número de instituições que declararam possuir processo de planejamento da contratação e de gestão de contratos foi muito baixo, revelando que a situação real em 2007 era, na realidade, ainda mais crítica que o quadro apontado no levantamento daquele ano.

Por outro lado, há sinais de iniciativas no sentido de reverter essa realidade. Houve evolução significativa no índice referente a planejamento estratégico institucional, o qual é pré-requisito para um planejamento estratégico de TI alinhado com o negócio, além de ser essencial para a definição de objetivos de desempenho. Além disso, o número de instituições que declararam possuir carreira própria de TI praticamente dobrou, alcançando 78%.

Tendo em vista esses primeiros resultados de evolução da governança de TI no setor público federal, mas reconhecendo que a tarefa está somente começando, é importante que o TCU permaneça no seu papel como indutor desse processo, como já tem feito por meio de fiscalizações, diálogos públicos, notas técnicas etc.".

3.3. Levantamento de informações de 2012

O objetivo do levantamento de 2012 foi acompanhar e manter a base de dados atualizada com a situação de governança de tecnologia da informação (TI) na Administração Pública Federal (APF), aprofundando o panorama traçado em 2010, materializado pelo Acórdão 2.308/2010-TCU-Plenário.

Durante a fase de planejamento, foram elaboradas 36 questões, subdivididas em 494 itens, contemplando as oito dimensões do GesPública (Decreto nº 5.378/2005): liderança, estratégias e planos, cidadãos, sociedade, informações e conhecimento, pessoas e processos, e resultados.

Foram utilizados, como referência para a elaboração do questionário, modelos de boas práticas reconhecidos internacionalmente, tais como o Cobit 5 (Control Objectives for Information and related Technology) (ITGI, 2012), a ABNT NBR ISO/IEC 27002 - segurança da informação (ABNT, 2005) e a ABNT NBR ISO/IEC 38500 - governança corporativa de TI (ABNT, 2009).

Foram selecionadas 350 instituições da APF, tendo como critério principal a representatividade no orçamento da União e a autonomia de governança de TI dessas organizações, mantidas as 301 avaliadas no levantamento anterior. Foram acrescentados os institutos federais de ciência e tecnologia, as unidades de segundo escalão do Ministério do Planejamento, Orçamento e Gestão e os órgãos de direção-geral e setorial do Exército Brasileiro.

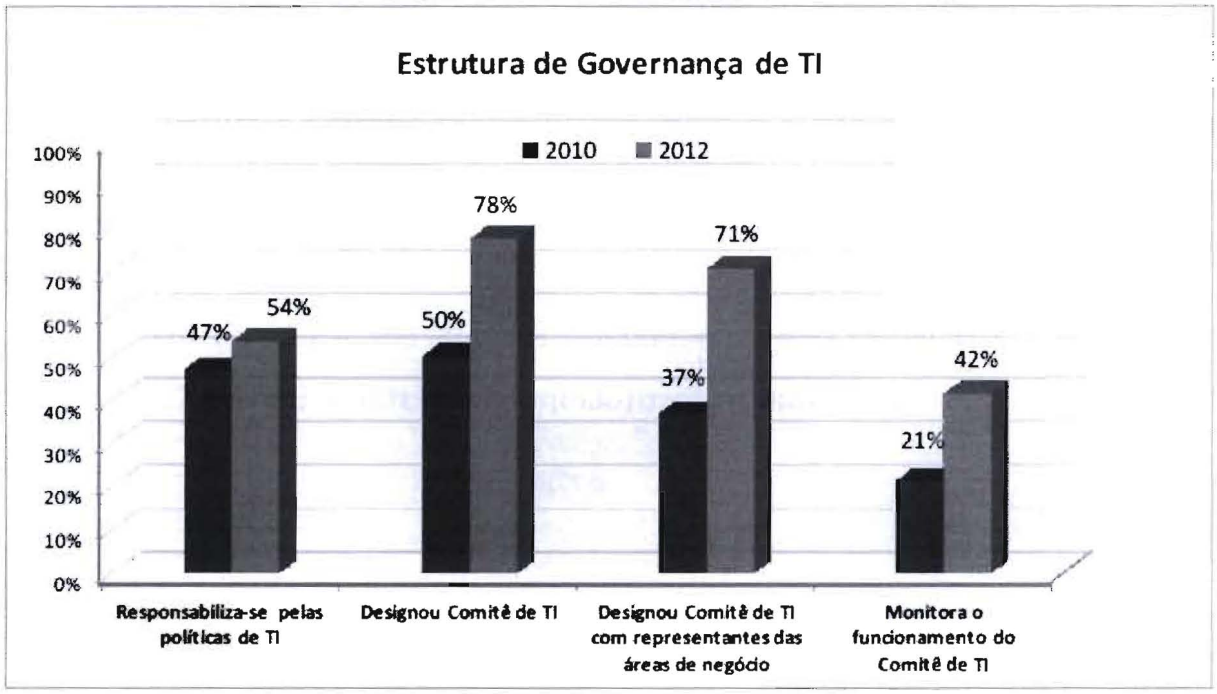
As instituições selecionadas foram combinadas em seis grupos, seguindo o mesmo critério utilizado na última avaliação, para facilitar a análise das informações:

- EXE-Dest: abrange as empresas públicas federais e as sociedades de economia mista;
- EXE-Sisp: abrange as instituições do Sistema de Administração dos Recursos de Informação e Informática (Sisp);
- JUD: abrange as instituições do Poder Judiciário;
- LEG: abrange as instituições do Poder Legislativo;
- MPU: abrange as instituições do Ministério Público da União (MPU);
- Outros: composto por instituições que não se enquadram nos segmentos anteriores, como é o caso da Associação das Pioneiras Sociais.

Até a conclusão do levantamento em análise, 337 instituições haviam atendido à solicitação de remessa de informações (Apêndice IV), restando 13 instituições inadimplentes

3.3.1. Estrutura de Governança de TI

Gráfico 21 - Comparativo da estrutura de Governança de TI



Fonte: Acórdão n.° 2.585/2012 - Tribunal de Contas da União

De acordo com os dados do levantamento, houve avanços com relação à situação encontrada em 2010. Em 2012, 54% das instituições declararam se responsabilizar pela avaliação e estabelecimento das referidas políticas (em 2010, 47% dos entrevistados, apenas, se declararam responsáveis).

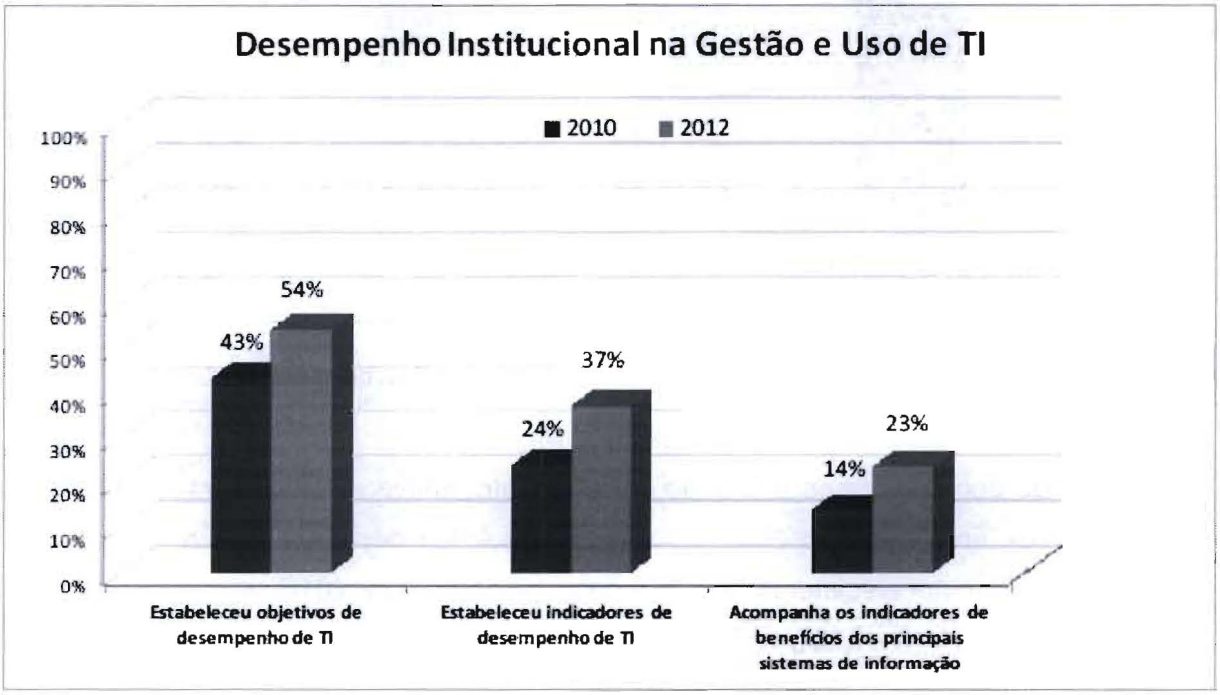
Verificou-se que 78% dos participantes declararam ter designado um comitê de TI, contra 50% em 2010. Contudo, segundo o TCU, ainda é preocupante, em face dos riscos decorrentes da inexistência desse tipo de comitê, que 22% dos avaliados ainda não o tenham estabelecido.

O gráfico demonstra também que, entre os que estabeleceram o comitê, 71% designaram representantes da área de negócio, o que representa evolução em relação a 2010, que indicava apenas 37%. Por outro lado, apenas 42% monitora o funcionamento do comitê, situação que indica melhora em relação ao levantamento anterior (21%), mas pouco significativa, haja vista que 58% das instituições ainda não acompanham e avaliam as atividades dos comitês.

De acordo com o Tribunal de Contas da União, "os dados levantados demonstram evolução da estrutura de governança de TI das instituições públicas federais, e sugerem que sua alta administração passou a ter melhor compreensão da importância dessa estrutura para o seu negócio. Contudo, ainda preocupa que 46% dos avaliados tenham declarado não se responsabilizar pelas políticas de TI, tendo em vista que essas políticas visam garantir que o uso da TI contribua para melhor desempenho da instituição".

3.3.2. Desempenho Institucional na Gestão e Uso de TI

Gráfico 22 - Desempenho Institucional em Gestão e Uso de TI



Fonte: Acórdão n.° 2.585/2012 - Tribunal de Contas da União

Verificou-se que 54% das instituições estabeleceram objetivos de desempenho de TI, contra 43% em 2010, revelando melhora em relação ao levantamento anterior. Entretanto, 46% de instituições que não definiram esses objetivos ainda são um percentual alto, levando em consideração o risco associado à ausência dessas diretrizes.

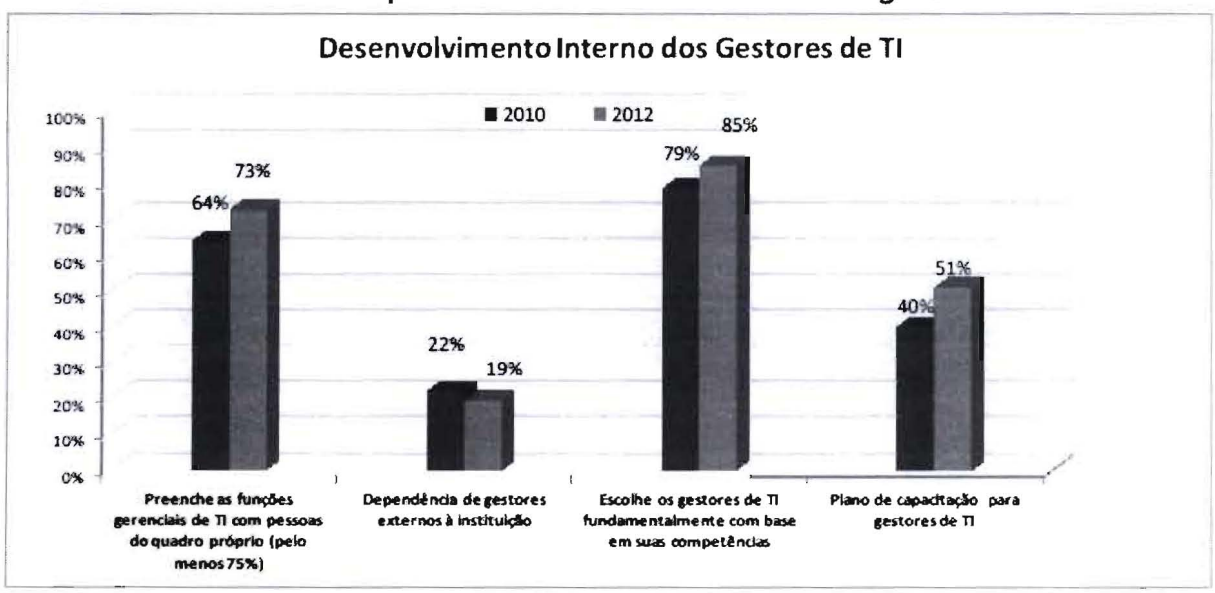
De acordo com o Tribunal, "a situação se agrava quando se observa que apenas 37% dos avaliados estabeleceram indicadores de desempenho e somente 23% acompanham os indicadores de benefícios dos principais sistemas de informação, embora esses percentuais sejam melhores do que os apurados em 2010, 24% e 14%, respectivamente".

Em suma, ainda segundo a Corte de Contas, "os números revelados sugerem que a maioria das instituições públicas federais tem dificuldade em perseguir seus objetivos, uma vez que nem chegam a definir os indicadores que serão a referência para avaliar o alcance deles. Além disso, poucos são os que tomam decisões com base nos benefícios de negócio oriundos de seus principais sistemas de informação. Dessa forma, sob a ótica da eficiência e da efetividade, o alcance dos resultados institucionais tende a ser prejudicado".

Por fim, o Tribunal concluiu que "diante dos dados apurados, pode-se afirmar que a situação identificada no presente levantamento evoluiu em relação ao cenário encontrado em 2010. Entretanto, a alta administração das instituições públicas, em geral, continua a não se preocupar com a gestão e o uso de TI, situação que pode comprometer o desempenho e, por consequência, o alcance dos objetivos institucionais. O quadro identificado reforça a necessidade de os órgãos governantes superiores continuarem a adotar medidas para ampliar o universo de instituições que atendam a recomendação constante do item 9.1 do Acórdão 2.308/2010-TCU-Plenário".

3.3.3. Desenvolvimento Interno de Gestores de TI

Gráfico 23 - Comparativo do desenvolvimento de gestores de TI



Fonte: Acórdão n.º 2.585/2012 - Tribunal de Contas da União

Verificou-se que 73% das instituições preenchem as funções gerenciais de TI com pessoas do próprio quadro, contra 64% em 2010. Consequentemente, percebeu-se redução

no percentual de organizações que dependem de gestores externos aos seus quadros (19%).

Apesar da melhora, segundo o TCU, "ainda é elevada a quantidade de instituições que recorrem a pessoas externas aos seus quadros para exercer funções gerenciais de TI, situação que eleva o risco de descontinuidade da gestão de TI".

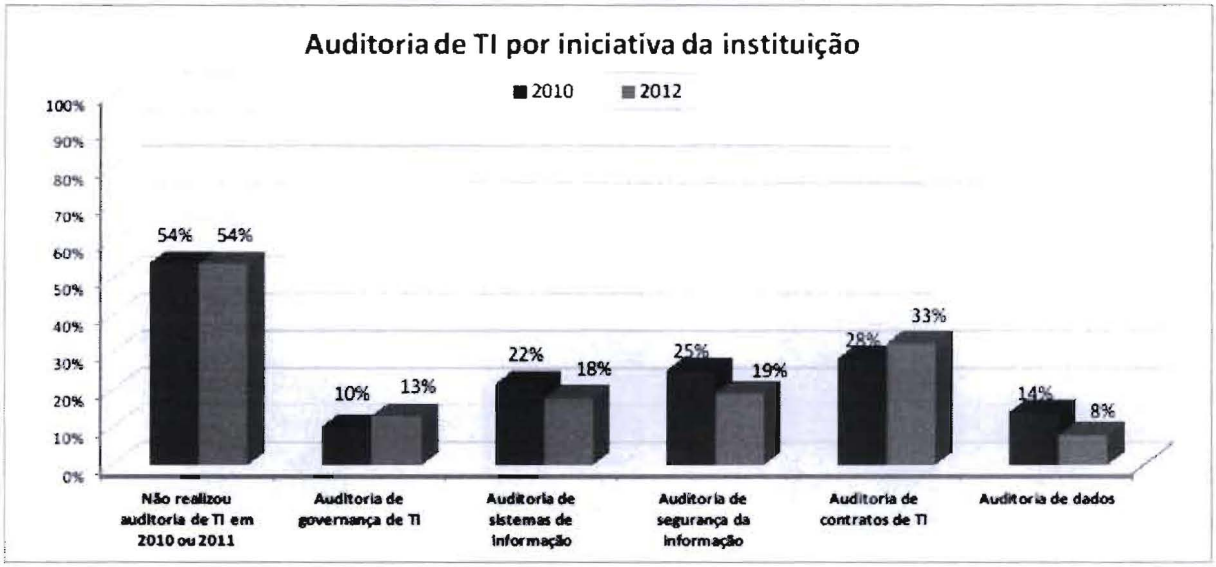
Com relação à escolha dos gestores de TI, 85% dos avaliados afirmaram que levam em consideração fundamentalmente suas competências. Porém, o fato de 15% de instituições não selecionarem seus gestores de TI com base em competências é preocupante.

Houve também evolução no percentual de instituições que possuem plano de capacitação para gestores de TI, 51% declaram possuí-lo.

Segundo o Tribunal, "o presente levantamento demonstrou evolução nos percentuais relacionados ao desenvolvimento interno dos gestores de TI em relação ao cenário identificado em 2010. Contudo, os resultados obtidos ainda não são os desejáveis, tendo em vista que algumas instituições continuam a preencher suas funções gerenciais de TI com pessoas estranhas ao seu quadro e, ainda mais grave, não selecionam essas pessoas com base nas competências exigidas para o exercício da função".

3.3.4. Auditoria de TI

Gráfico 24 - Comparativo de realização de auditoria de TI



Fonte: Acórdão n.° 2.585/2012 - Tribunal de Contas da União

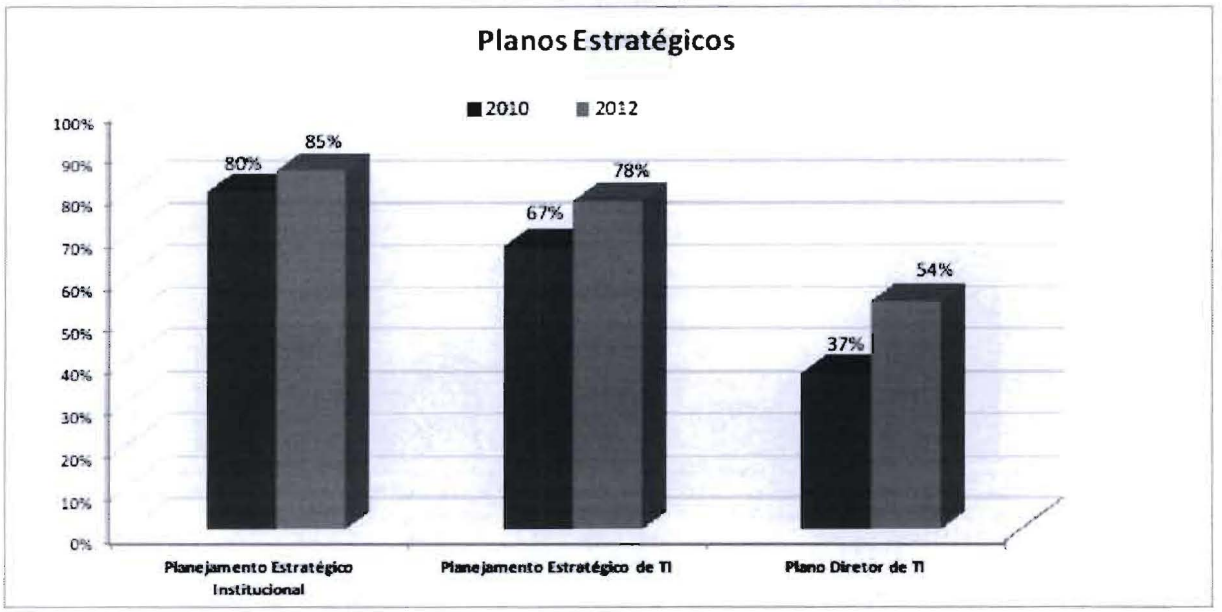
Segundo os dados coletados, a situação permaneceu inalterada no que se refere ao percentual de instituições que não realizaram auditoria de TI no intervalo entre dois levantamentos subsequentes, com a manutenção do percentual de 54%.

De acordo com o TCU, "a falta de estrutura das auditorias internas nas instituições públicas federais, especialmente a ausência de pessoal com conhecimento especializado para realizar esse tipo de trabalho, apesar de não impedir a realização de auditorias, contribui significativamente para esse cenário".

Verificou-se, também, discreto aumento nos percentuais de realização de auditoria de governança e de contratos de TI em 2012. Nos demais tipos de auditoria, percebeu-se pequena queda dos percentuais em relação a 2010.

3.3.5. Planejamento Estratégico Institucional e de TI

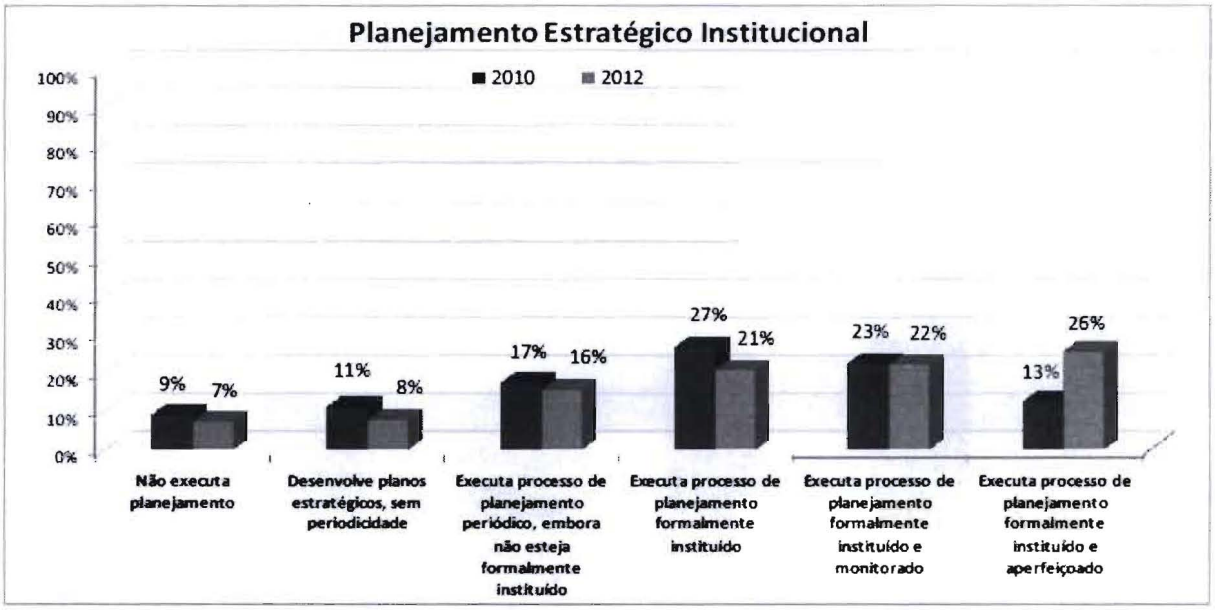
Gráfico 25 - Comparativo de planos estratégicos



Fonte: Acórdão n.° 2.585/2012 - Tribunal de Contas da União

Os resultados apurados indicam evolução no quantitativo de instituições que elaboram seus instrumentos de planejamento estratégico. No presente levantamento, 85% das instituições afirmaram realizar planejamento estratégico institucional, contra 80% no levantamento de 2010. Em relação ao planejamento estratégico de TI, o índice subiu de 67% para 78% na avaliação corrente. Por outro lado, no caso do plano diretor de TI, a evolução mostrou-se também favorável, haja vista ter passado de 37% para 54% o percentual de instituições que elaboram esse plano.

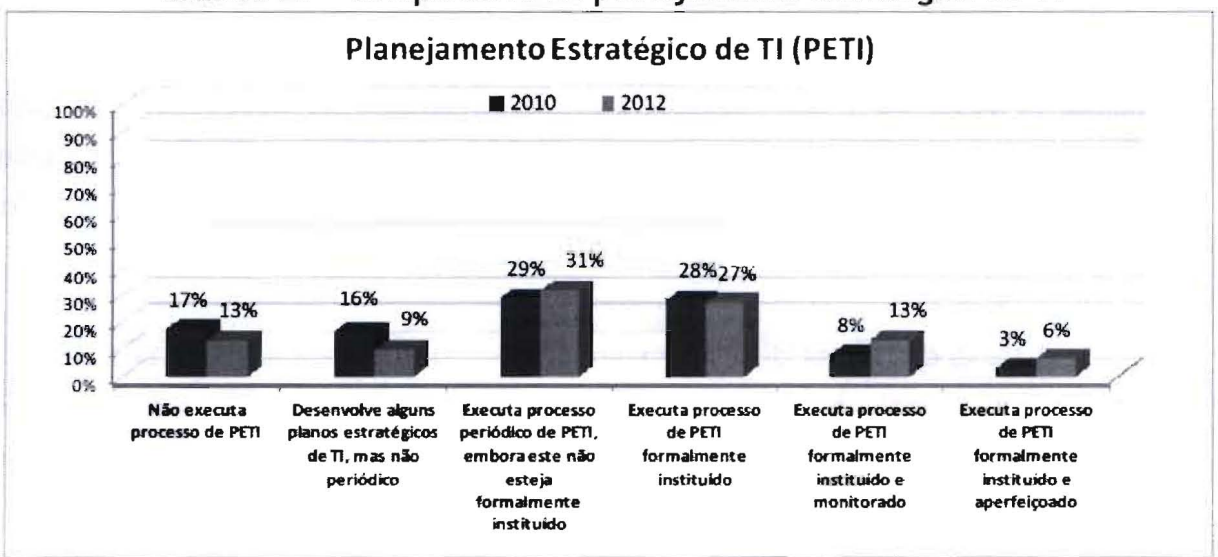
Gráfico 26 - Comparativo de planejamento estratégico institucional



Fonte: Acórdão n.º 2.585/2012 - Tribunal de Contas da União

A figura acima demonstra migração positiva para níveis de capacidade mais especializados. Verificou-se, por exemplo, que o índice de instituições que executam processo de planejamento formalmente instituído e aperfeiçoado subiu de 13% para 26% no presente levantamento.

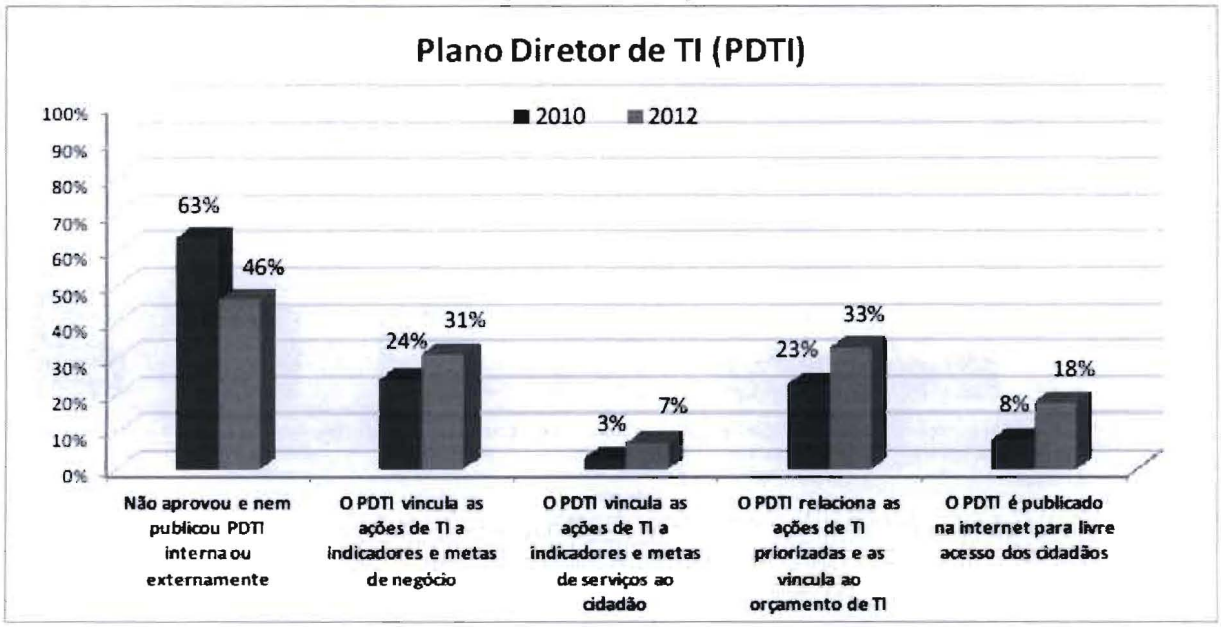
Gráfico 27 - Comparativo de planejamento estratégico de TI



Fonte: Acórdão n.º 2.585/2012 - Tribunal de Contas da União

Constatou-se, também, que, em 2010, por exemplo, 16% das instituições desenvolviam planos estratégicos de TI, mas sem periodicidade, e apenas 3% estavam em nível aperfeiçoado. Esses mesmos percentuais, em 2012, correspondem a 9% e 6%, respectivamente.

Gráfico 28 - Comparativo de plano diretor de TI



Fonte: Acórdão n.° 2.585/2012 - Tribunal de Contas da União

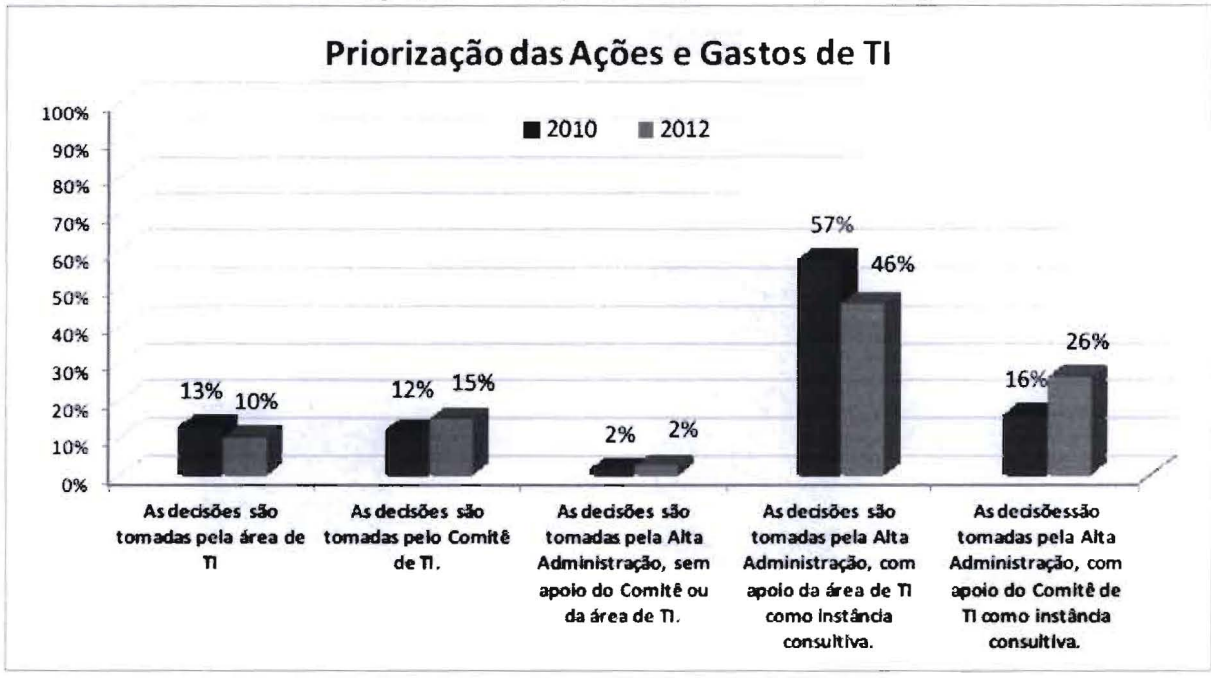
Com relação ao plano diretor de TI (PDTI), os resultados também revelam melhora na elaboração desse instrumento. Verificou-se, por exemplo, que 31% dos avaliados declaram vincular, no PDTI, as ações de TI a indicadores e metas de negócio, situação melhor do que a identificada em 2010 (24%), mas distante do desejável.

De acordo com o TCU, "percebe-se, com base no percentual de organizações que vincula as ações de TI a indicadores e metas de serviços ao cidadão - 7% no presente levantamento contra 3% no anterior -, que as instituições ainda têm dificuldade em identificar, ou relacionar, a contribuição das ações de TI no âmbito da prestação dos serviços finalísticos institucionais".

A Corte de Contas dispõe também que "em que pese a melhoria dos percentuais, ainda é preocupante que muitas instituições não executem processo de planejamento estratégico, sobretudo porque as contratações de TI devem ser planejadas em harmonia com os instrumentos que derivam desse processo (...)".

3.3.6. Priorização das Ações e Gastos de TI

Gráfico 29 - Comparativo da priorização das ações e gastos de TI



Fonte: Acórdão n.° 2.585/2012 - Tribunal de Contas da União

O Tribunal de Contas da União verificou que, com relação ao percentual de instituições cujas decisões são tomadas pela alta administração, a situação permaneceu praticamente inalterada (em torno de 75% em ambos os levantamentos).

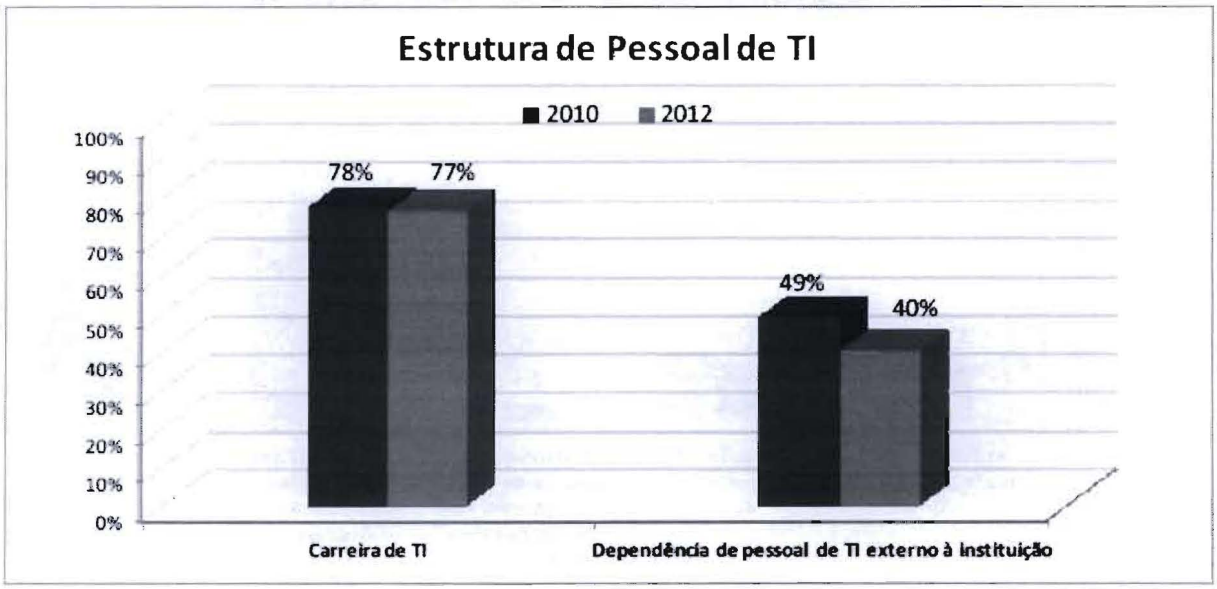
A quantidade de instituições cuja área de TI é responsável pelas decisões de priorização das ações e gastos de TI diminuiu timidamente, passando de 13% para 10%, número que, segundo o Tribunal, ainda preocupa, visto que, além de ser atribuição do dirigente máximo da instituição, a área de TI pode não ter autonomia ou conhecimento necessário para selecionar as ações prioritárias para o negócio.

Observou-se discreto aumento na quantidade de instituições cujas decisões são tomadas pelo comitê de TI – de 12% para 15%.

De forma geral, percebeu-se tendência de migração da responsabilidade pelas decisões acerca de investimentos em TI da área de tecnologia para o comitê de TI. A participação da área de tecnologia nessas decisões, de forma direta ou por consulta, reduziu-se em 13% (3% mais 10%), enquanto a participação dos comitês de TI nessas decisões, também de forma direta ou por consulta, cresceu os mesmos 13% (3% mais 10%).

3.3.7. Estrutura de Pessoal de TI

Gráfico 30 - Comparativo da estrutura de pessoal de TI



Fonte: Acórdão n.° 2.585/2012 - Tribunal de Contas da União

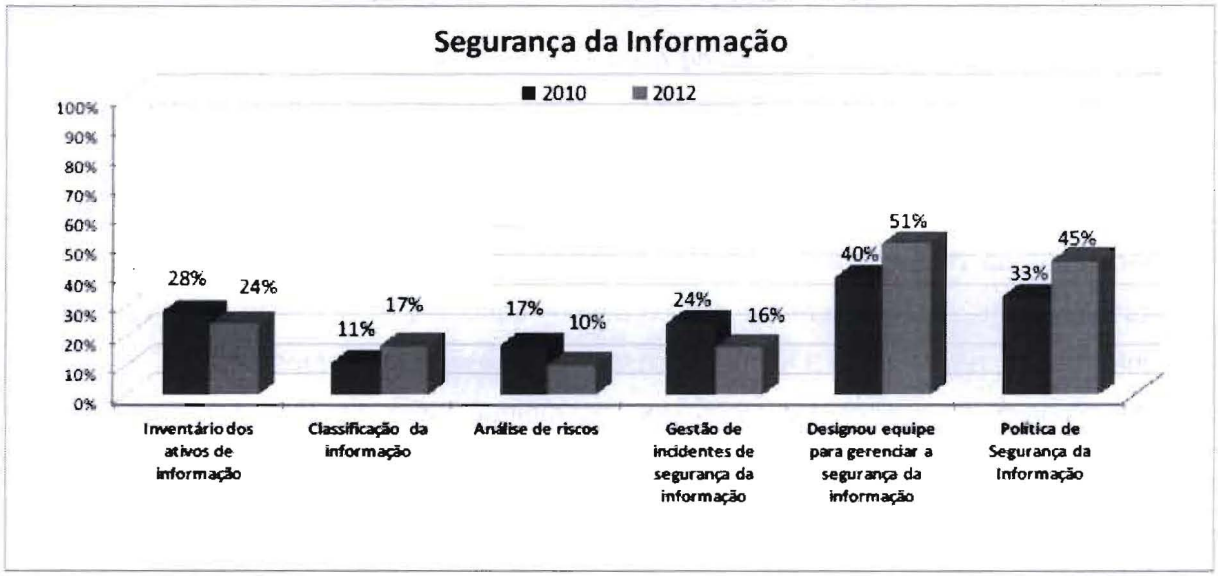
Verificou-se, com base nos resultados apurados, que a quantidade de instituições com carreira própria de TI permaneceu estável, registrando 77% no presente levantamento contra 78% no anterior.

Quanto à dependência de pessoal externo, verificou-se redução desejável no percentual, com decréscimo de nove pontos, chegando aos 40% em 2012.

De acordo com o TCU, "os dados sugerem, portanto, que a maioria das instituições públicas federais (60%) não se encontra em situação de dependência de pessoas externas aos seus quadros, o que possibilita a internalização de conhecimento do negócio e, em especial, a continuidade das ações e projetos de TI".

3.3.8. Segurança da Informação

Gráfico 31 - Comparativo da situação de segurança da informação



Fonte: Acórdão n.° 2.585/2012 - Tribunal de Contas da União

Verificou-se razoável evolução nos percentuais relacionados à designação de equipe para gerenciamento da segurança da informação e à formalização de política de segurança da informação (PSI), que variaram positivamente onze e doze pontos percentuais, respectivamente. Apesar da evolução, segundo o TCU, a situação ainda preocupa, principalmente em relação à PSI, haja vista que a ausência dessa política pode implicar em procedimentos não padronizados relativos à segurança; deficiência nos controles de segurança; dificuldade de responsabilização em incidentes de segurança; risco de acessos não autorizados e de vazamento de dados e informações; entre outros.

Observou-se também ligeira evolução no percentual de instituições que possuem processo de classificação das informações, que saltou de 11% para 17%. Entretanto, esse percentual ainda é baixo, sobretudo considerando o advento da Lei nº 12.527/2011, que regula o acesso a informações mantidas pelo Estado, haja vista que a ausência de classificação pode implicar em tratamento inadequado da informação, como a divulgação ostensiva de dados não públicos.

Por outro lado, a apuração revelou redução dos percentuais relativos aos seguintes processos: inventário de ativos de informação, análise de riscos e gestão de incidentes. Segundo o Tribunal de Contas da União, "essa queda não se traduz necessariamente em retrocesso, mas, como colocado no levantamento anterior, no amadurecimento dos gestores

de TI no sentido de compreender melhor os conceitos relacionados à segurança da informação".

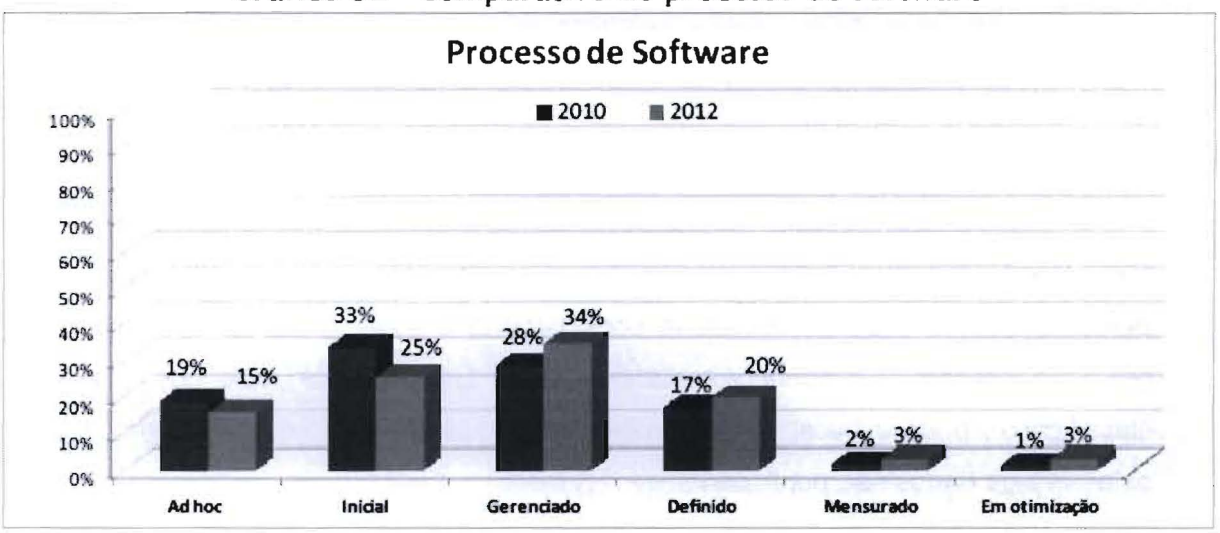
Ainda segundo a Corte, causa preocupação especial o baixo percentual de instituições que realizam análise de risco, que passou de 17% para 10%. Ou seja, 90% das instituições públicas federais ainda não realizam esse tipo de análise.

O TCU dispõe que "deve-se ressaltar que um processo de análise de riscos é indicador da maturidade da gestão de determinada instituição. De início, esse processo recebe como insumos o mapa dos processos críticos e o inventário de ativos, físicos e de informação, necessários a esses processos. Sem esses elementos básicos, qualquer gestão de riscos é, na melhor das hipóteses, incompleta. Além disso, o resultado da análise de riscos é insumo essencial para outros processos, como a gestão de continuidade do negócio".

Dessa forma, o TCU conclui que, dado que apenas 10% das organizações declararam realizar análise de riscos, a gestão da tecnologia da informação ainda se encontra em nível baixo de maturidade na Administração Pública.

3.3.9. Processo de Software

Gráfico 32 - Comparativo de processo de software



Fonte: Acórdão n.° 2.585/2012 - Tribunal de Contas da União

Segundo o TCU, "o processo de software, em suma, é um conjunto de atividades, métodos e procedimentos a serem seguidos no desenvolvimento e manutenção do software, que visa monitorar e mitigar os riscos associados às atividades, garantindo a entrega do produto projetado em nível de qualidade aceitável. Nessa questão, buscou-se avaliar o nível de capacidade em que se enquadra o processo de software da instituição, com base nas definições da norma ABNT NBR ISO/IEC 15504".

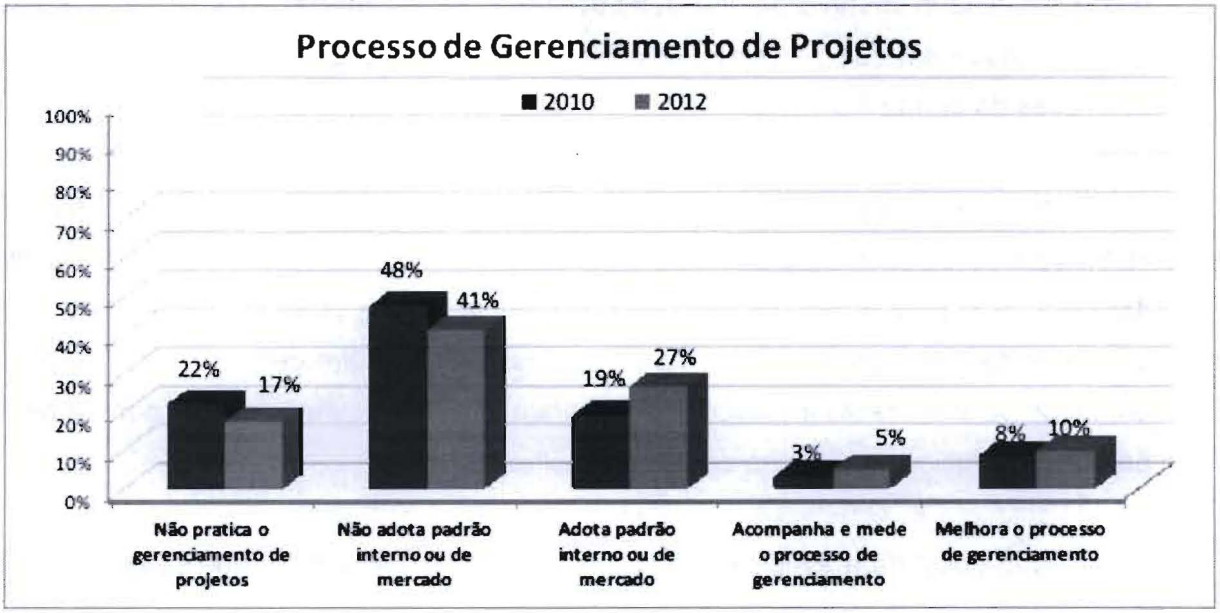
No que tange aos resultados apurados, percebeu-se melhora no percentual de instituições que possuem processo de software, no mínimo, gerenciado, o qual saltou de 48% em 2010 para 60% no presente levantamento. Nesse universo, verificou-se migração desejável de instituições para o nível de processo de software definido - de 17% para 20% em 2012, ou seja, essas instituições declararam ter procedimentos gerenciados constituindo padrões institucionais capazes de atingir resultados.

Não obstante a evolução, 40% das instituições declararam que seus softwares são desenvolvidos ou mantidos sem a orientação de um processo, entre as quais, 15% não adotam sequer conceitos de qualidade (Ad Hoc). De acordo com o Tribunal de Contas da União, "esse quadro revela o risco a que essas instituições estão submetidas quando optam por terceirizar essas atividades, haja vista que a ausência de processo de software tende a inviabilizar a avaliação dos serviços contratados, o que possivelmente prejudicará a qualidade do produto gerado, podendo até comprometê-lo".

Ainda segundo o Tribunal, "cabe destacar que os contratos de desenvolvimento de software, com base no art. 6º, inciso IX, da Lei nº 8.666/93, devem especificar as atividades e artefatos presentes em cada fase do projeto. O atendimento dessa exigência legal fica praticamente inviável diante da inexistência de processo de software. Nesse contexto, pode-se presumir que muitas instituições públicas federais podem estar incorrendo em irregularidades nas contratações dessa natureza".

3.3.10. Processo de Gerenciamento de Projetos

Gráfico 33 - Comparativo do processo de gerenciamento de projetos



Fonte: Acórdão n.° 2.585/2012 - Tribunal de Contas da União

Os resultados obtidos revelam que mais da metade das instituições (58%) não adota processo de gestão de projetos baseado em padrão interno ou de mercado. Em 2010, esse percentual era 70%, o que demonstra evolução da situação nos últimos dois anos. Chama à atenção que 17% das instituições não pratiquem qualquer gerenciamento de projetos, mesmo diante da complexidade que envolve o desenvolvimento de serviços e produtos de TI.

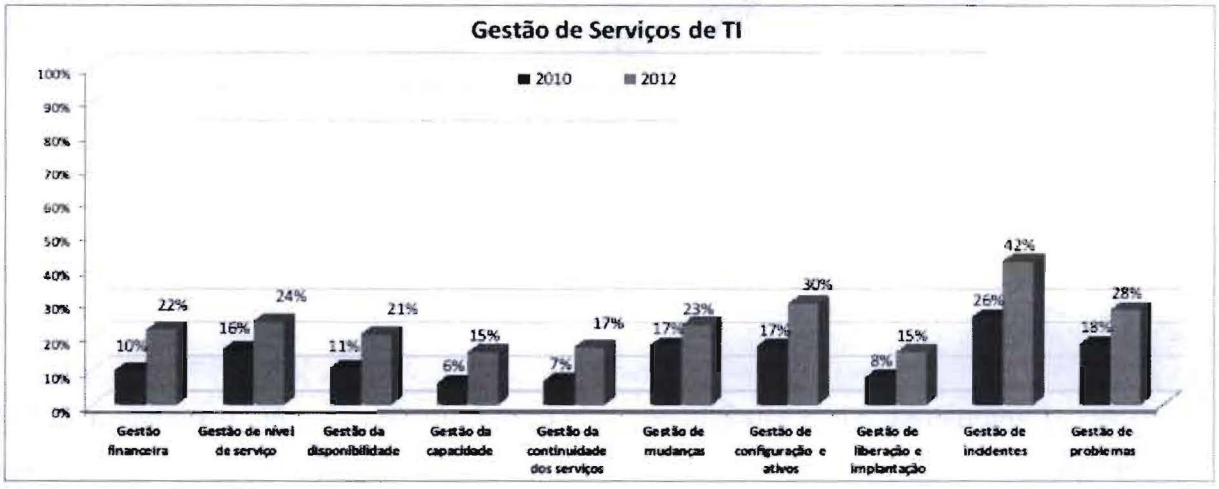
Segundo o TCU, "a ausência desse tipo de processo tem impacto direto na taxa de sucesso dos projetos institucionais. Projetos de TI possuem riscos tão conhecidos, que chegam a ser prováveis em muitos casos, como o aumento dos custos inicialmente previstos e a dilação do prazo de entrega do produto. Não raro, o projeto fracassa no alcance de seus objetivos, e compromete ações institucionais. Enfim, uma instituição que não gerencia seus projetos adequadamente sofre elevado risco de ter desempenho insatisfatório".

Dentre as instituições que declararam adotar processo de gerenciamento de projetos baseado em um padrão, tem-se que apenas 5% acompanham e mensuram esse processo, e somente 10% buscam melhorá-lo, situação que ficou praticamente inerte em relação ao levantamento anterior, cujos resultados foram 3% e 8%, respectivamente.

De acordo com o TCU, "as informações colhidas sugerem que há tendência positiva de amadurecimento da cultura da gestão de projetos. Baixo nível de capacidade desse quesito sugere baixo nível de maturidade na gestão de TI, situação que ainda persiste em mais da metade das instituições".

3.3.11. Gestão de Serviços de TI

Gráfico 34 - Comparativo do processo de gestão de serviços de TI



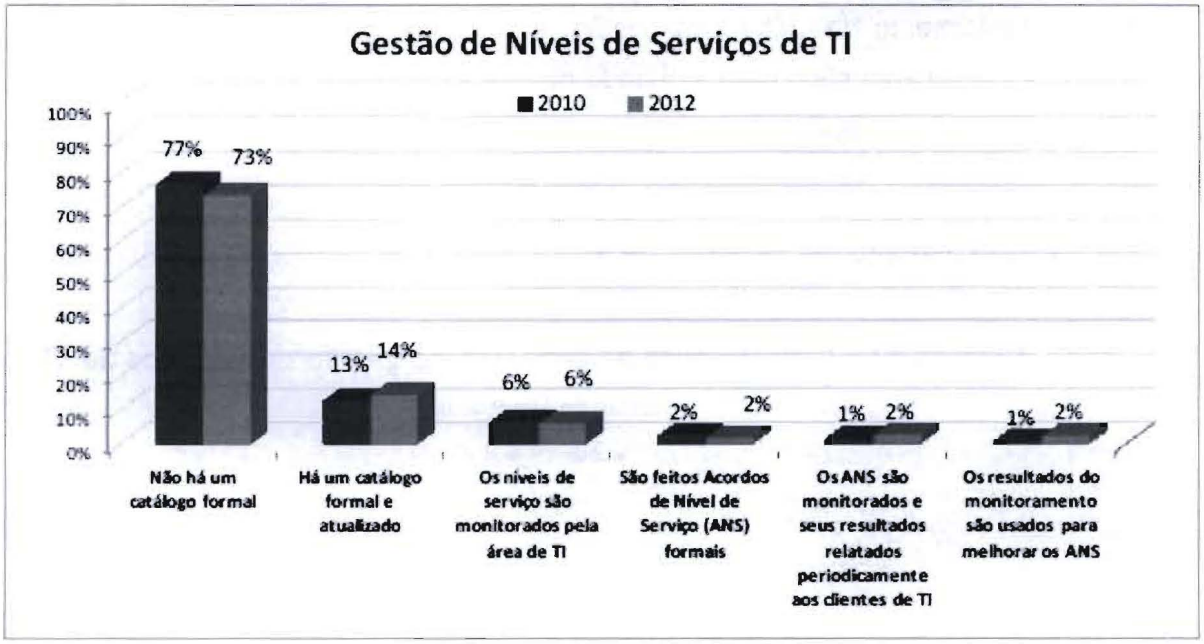
Fonte: Acórdão n.º 2.585/2012 - Tribunal de Contas da União

Os dados levantados indicaram melhoria em todos os percentuais vinculados à gestão de serviços de TI, em relação ao levantamento de 2010, com exceção da gestão de incidentes de segurança da informação, conforme apresentado anteriormente.

De acordo com o TCU, "em que pese a melhoria apurada, o percentual de instituições que praticam gestão de serviço adequada ainda é baixo".

Além da verificação acerca da existência de processos de gestão de serviço, avaliou-se também a gestão dos níveis de serviços prestados aos clientes.

Gráfico 35 - Comparativo do processo de gestão de níveis de serviços de TI



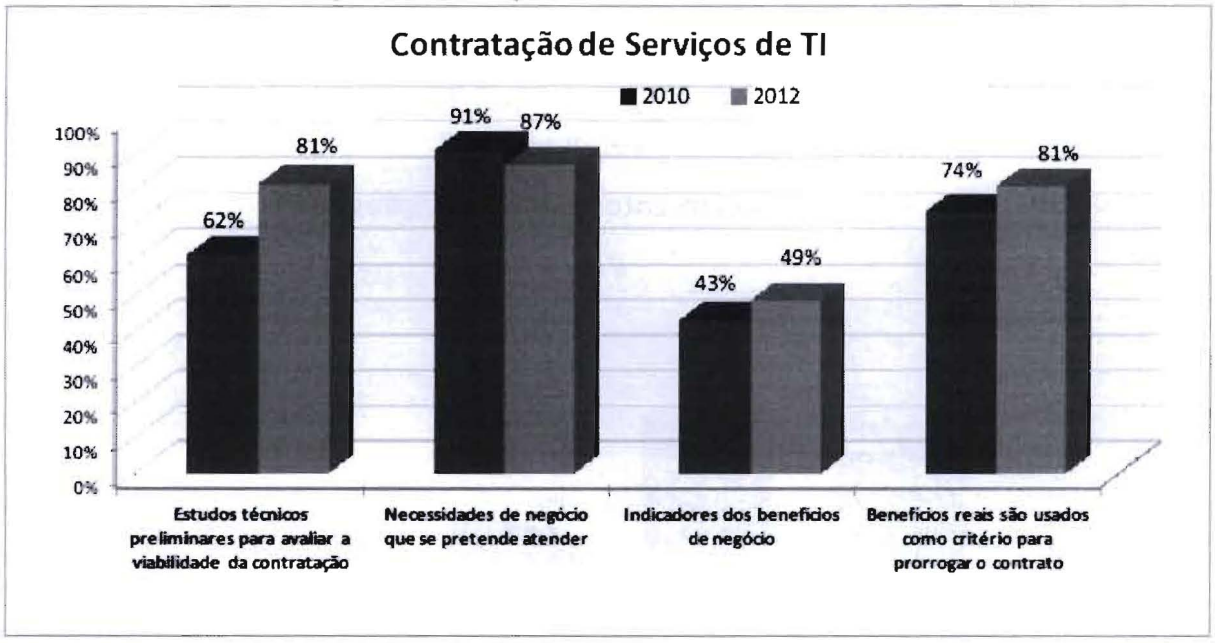
Fonte: Acórdão n.° 2.585/2012 - Tribunal de Contas da União

Percebeu-se que a situação continua crítica. Verificou-se, por exemplo, que 73% das instituições não possuem catálogo dos serviços de TI oferecidos aos clientes. Em um cenário ainda mais crítico, observou-se que 98% das organizações públicas federais sequer estabelecem acordos de nível de serviços (ANS) entre a área de TI e suas áreas clientes, situação que prejudica a avaliação dos serviços de TI e tende a afetar a qualidade dos resultados esperados.

De acordo com o Tribunal de Contas da União, "uma interpretação possível para a situação seria a falta de prioridade para a formalização desse tipo de acordo. É difícil estabelecer um acordo com a área de TI acerca da disponibilidade de determinados serviços, se o processo de gestão de disponibilidade (em 21%) não está implantado. Ou seja, é natural que os esforços sejam focados no estabelecimento de processos mais elementares da gestão".

3.3.12. Processo de Contratação de TI

Gráfico 36 - Comparativo do processo de contratação de serviços de TI



Fonte: Acórdão n.° 2.585/2012 - Tribunal de Contas da União

Observou-se evolução na quantidade de instituições que realiza estudos preliminares para avaliar a viabilidade da contratação. O respectivo percentual, que era 62% em 2010, elevou-se para 81% no presente levantamento.

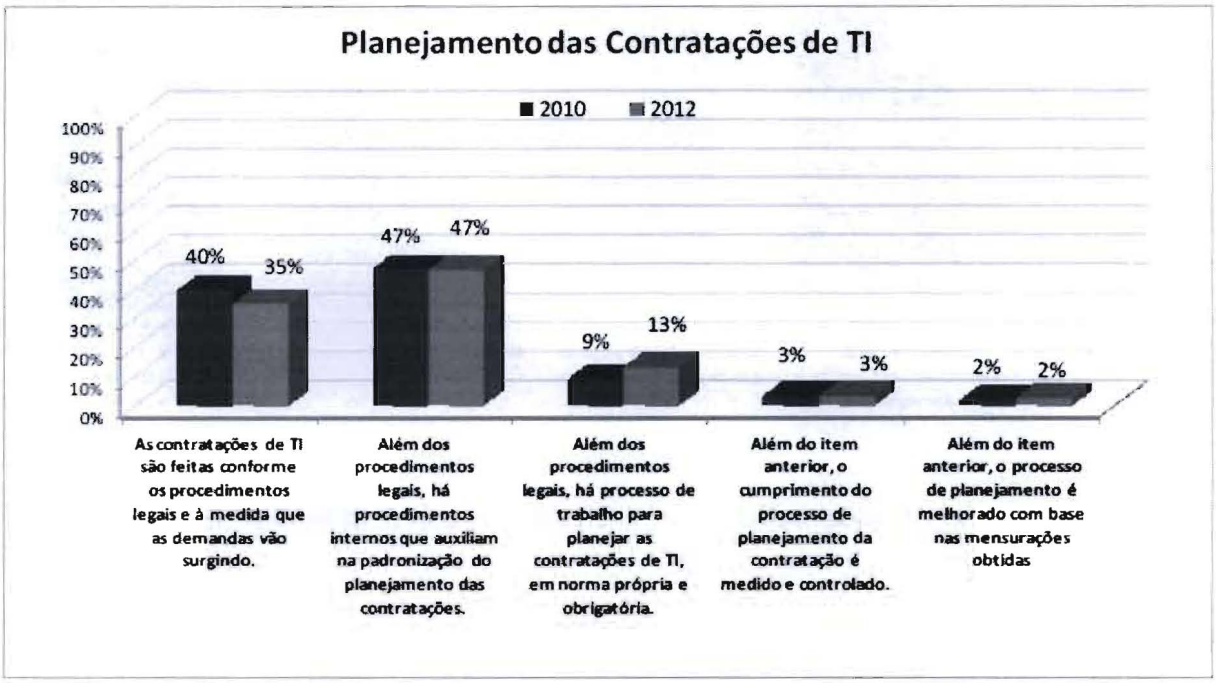
O percentual de instituições que explicitam nos autos os indicadores dos benefícios de negócios a serem alcançados também apresentou evolução, subindo seis pontos percentuais – de 43% para 49%. No mesmo sentido, o percentual de instituições que declararam levar em consideração os benefícios reais já obtidos para prorrogar os contratos de TI apresentou melhora, ao passar de 74% em 2010 para 81% no levantamento corrente.

Diferentemente dos demais percentuais, a quantidade de instituições que explicitam nos autos as necessidades de negócio que se pretende atender com a contratação passou de 91% para 87% em 2012. Esse decréscimo, segundo o TCU, pode ser explicado por uma melhor compreensão por parte da Administração dos conceitos envolvidos na resposta dessa questão.

No que se refere ao planejamento das contratações de TI, verificou-se, a partir da figura abaixo, que houve melhora da situação em relação ao levantamento anterior.

Observou-se, inicialmente, que apenas 18% das instituições possuem processo de planejamento formalizado, considerando nessa situação as instituições que, no mínimo, possuem norma própria e de cumprimento obrigatório. Em 2010, esse percentual era de 14%.

Gráfico 37 - Comparativo do processo de planejamento de contratação de serviços de TI



Fonte: Acórdão n.° 2.585/2012 - Tribunal de Contas da União

Ressalta-se, também, a baixa quantidade de instituições que têm processo de planejamento mais especializado - medido e controlado ou melhorado com base nas medições. Os resultados demonstraram que apenas 3% medem e controlam seu processo. Percentual semelhante se aplica àqueles que o melhoram com base nas medições realizadas. A situação manteve-se em patamares similares ao do último levantamento, cujos índices correspondiam a 3% e 2%, respectivamente.

3.3.13. Gestão de Contratos de TI

Gráfico 38 - Comparativo do processo de gestão de contratos de TI

Fonte: Acórdão n.° 2.585/2012 - Tribunal de Contas da União

Verificou-se que o cenário de 2012 não variou em relação ao identificado em 2010, mantendo-se o baixo percentual de 31% de instituições que possuem processo, no mínimo, formalizado de gestão de contratos de TI. Dentre essas instituições, apenas 5% mede e controla esse processo, percentual praticamente igual ao apurado no último levantamento (6%). O quadro também ficou inalterado em relação ao percentual de instituições que melhoram seus processos com base nas mensurações realizadas, com apenas 3% em ambos os levantamentos.

Enfim, 69% das instituições declararam não possuir processo de gestão de contrato aprovado e publicado em norma própria e de cumprimento obrigatório, situação que eleva o risco de efeitos negativos na execução de seus contratos de serviços de TI, sobretudo pela ausência de padronização de procedimentos, permitindo que gestores e fiscais de contrato possam adotar condutas não objetivas. Da mesma forma, o quadro praticamente não se alterou em relação ao levantamento anterior.

Gráfico 39 - Comparativo do suporte à Gestão e Fiscalização de Contratos de TI

Fonte: Acórdão n.° 2.585/2012 - Tribunal de Contas da União

Observou-se que 68% das instituições avaliadas designam formalmente gestor de contrato, o que praticamente não se modificou em relação ao levantamento de 2010, cujo percentual era 64%. Por outro lado, elevou-se a quantidade de instituições que designam fiscais para seus contratos de serviços de TI, passando de 67% para 79%.

Por fim, de acordo com o TCU, "infere-se do gráfico que mais de 70% das instituições não treinam nem possuem programa de capacitação para o exercício das funções de gestor e de fiscal. Esse quadro indica a pouca preocupação que essas organizações públicas têm com a capacitação das pessoas que recebem a missão de avaliar e garantir a correta execução contratual e, ao mesmo tempo, sugere o nível de despreparo dessas pessoas para o exercício das respectivas funções".

3.3.14. Conclusão

Segundo o Tribunal de Contas da União: "o levantamento de governança de TI 2012 revelou, de forma geral, melhoria da situação em relação ao levantamento de 2010. Contudo, ainda há instituições na faixa inicial de governança de TI, o que está distante do aceitável, tendo como referência os modelos de boas práticas de governança de TI e a legislação e a jurisprudência vigentes".

Diante do cenário levantado, de acordo com o Tribunal, "percebe-se que há espaço para melhorias, o que justifica a continuidade das ações do TCU no sentido de alavancar a governança de TI na APF, e, sobretudo, dos levantamentos de governança de TI, que, além da ação indutora, permitem verificar a evolução da situação ao longo de um período e direcionar as ações posteriores".

Em 2010, sinais de melhoria já haviam sido detectados, mas em poucos aspectos, particularmente no aumento da quantidade de instituições que tinham processo de planejamento estratégico institucional e que tinham adotado carreira de TI, o que prenunciava melhorias no futuro. Em 2012, foram detectadas melhorias em vários dos aspectos avaliados e foi iniciada mensuração de resultados de TI. Novos trabalhos de auditoria poderão confirmar se tais melhorias são consistentes e sustentáveis e se as instituições públicas efetivamente aumentarão os benefícios de TI dirigidos à sociedade brasileira.

4. Avanços e Desafios

De acordo com os estudos do Tribunal de Contas da União, percebe-se que a situação da Governança de TI na Administração Pública vem melhorando a cada monitoramento, ainda que a passos lentos. Ainda de acordo com os monitoramentos realizados pelo TCU, 85% das instituições já possuem um Planejamento Estratégico Institucional, e 78% já possuem um Planejamento Estratégico de TI. A criação de carreiras específicas de TI e o aumento dos controles também mostram avanços no sentido de implantar uma governança na área de Tecnologia da Informação.

No entanto, esses avanços ainda são pequenos em relação ao volume de investimentos e à importância da área de TI no negócio das organizações. A falta de processos e de controles internos na área ainda é evidente, segundo os dados dos monitoramentos.

O maior desafio da Administração Pública ainda é instituir uma cultura de governança e controle na alta administração dos órgãos e empresas públicas. Conforme visto nos relatórios da Corte de Contas, apenas 37% dos avaliados estabeleceram indicadores de desempenho até o último monitoramento, e apenas 23% acompanham os indicadores de benefício dos principais sistemas de informação. Ainda, apenas 54% dos pesquisados declarou que a alta administração se responsabiliza pelas políticas de TI.

Ressalta-se, também, a gestão da segurança da informação, que teve poucos avanços desde o primeiro levantamento, em 2007. No último monitoramento, em 2012, menos da metade das instituições pesquisadas possuíam uma Política de Segurança da Informação. Essa política é vital para a garantia da segurança da informação, e deve envolver outras áreas além da TI, para garantir que todos aqueles que lidem com as informações dentro da organização sigam o mesmo padrão para garantir a segurança dos dados. Esse é um desafio relativamente simples de ser resolvido, pois não precisa de grandes investimentos, apenas de boa vontade e comprometimento da alta direção e dos demais envolvidos. Dentro ainda do quesito Segurança da Informação, temos a Classificação da Informação. De acordo com o monitoramento do TCU, 83% das instituições não classificam suas informações em diferentes níveis de sigilo de forma sistemática e organizada.

Outra questão importante é a falta de auditorias de TI nas instituições. De acordo com o estudo, 54% dos pesquisados declarou não ter realizado auditorias de TI nos anos de 2010 e 2011. Novamente, ressalta-se o volume de investimentos e a dependência das organizações em relação aos sistemas informatizados. Quando bilhões de reais são investidos em sistemas críticos para as instituições, é alarmante saber que mais da metade dos órgãos e empresas públicas não realiza auditorias nesses sistemas. Há também o risco para a continuidade do negócio, pois não há controles sobre os processos da área de TI, e o risco de desvio de dinheiro e danos ao erário, sejam esses causados de forma voluntária ou não.

5. Conclusão

Verificou-se, a partir dos dados levantados pelo Tribunal de Contas da União, o estágio atual de Governança de TI nas principais instituições públicas do Brasil. Percebeu-se uma melhora em vários pontos, em especial uma maior preocupação com o planejamento e com a gestão da área de Tecnologia da Informação.

A própria realização do estudo foi um fator de fomento a esse aumento do planejamento. A partir da realização do primeiro levantamento de informações, o tema Governança de TI passou a fazer parte da pauta de muitas instituições que antes não tinham sequer conhecimento da existência desse assunto. De 2007 para cá, várias instituições passaram a se preocupar em ter um maior controle sobre os seus processos de trabalho ligados à área de TI.

Ainda assim, verifica-se que a maior dificuldade ainda é a mesma mostrada na literatura sobre ou tema, ou seja, a mudança de cultura nas instituições, especialmente convencer a alta administração que a Governança de TI deve partir dela mesma, e não dos gestores da área de TI. Sem o apoio e o patrocínio da alta administração, é praticamente impossível implantar a Governança de TI.

Verificou-se também que ainda há poucos profissionais capacitados a serem gestores ou auditores na área de TI. Há uma grande preocupação em ter um corpo com conhecimentos técnicos sobre a área, mas há pouco investimento na capacitação de profissionais para planejar, controlar e gerir os processos de TI. Uma vez que a maioria dos órgãos e empresas terceiriza a execução dos trabalhos de TI, deveria haver um foco maior nas competências de gerenciamento e controle, em especial em relação aos contratos de TI.

Vale lembrar, ainda, que os resultados do levantamento realizado pelo Tribunal de Contas se basearam apenas nas respostas fornecidas pelas próprias instituições. Não foi escopo dos relatórios a verificação dos índices reais associados aos indicadores. Ainda que tenha sido pedido o envio de documentos comprobatórios das situações informadas, tais documentos não foram conferidos quanto a seu conteúdo. Dessa forma, os índices presentes nos monitoramentos podem não refletir a situação real dos órgãos, podendo estar superdimensionado.

Por fim, é possível ver que ainda há um longo caminho a ser trilhado pela Administração Pública para alcançar um nível mínimo de maturidade em relação à Governança de TI. No entanto, esse processo já foi iniciado, e está sendo acompanhado e incentivado pelo Tribunal de Contas da União, tornando possível que exista, no futuro, uma otimização na utilização dos recursos públicos e uma melhoria na qualidade dos serviços prestados à população.

Referências Bibliográficas

1. ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 38500:** Governança corporativa de tecnologia da informação. Rio de Janeiro, 2009.
2. BRASIL. Constituição (1988). **Constituição da República Federativa do Brasil**. Brasília, DF: Senado, 1988.
3. BRASIL, Lei n.º 8.666, de 21 de junho de 1993. Regulamenta o art. 37, inciso XXI, da Constituição Federal, institui normas para licitações e contratos da Administração Pública e dá outras providências. **Diário Oficial da União**, Brasília, DF, 22 ago. 1993. p. 8269.
4. BRASIL. Tribunal de Contas da União. **Acórdão n.º 1.603/2008**. Plenário. Relator: Ministro Guilherme Palmeira. Processo TCU 008.308/2007-1. Ata 32/2008. Sessão de 13/08/2008. Disponível em: http://portal2.tcu.gov.br/portal/page/portal/TCU/comunidades/tecnologia_informacao/pesquisas_governanca/D75C7DF1F44EB21CE040010A890070EC. Acesso em 12 nov. 2013.
5. BRASIL. Tribunal de Contas da União. **Acórdão n.º 2.308/2010**. Plenário. Relator: Ministro Aroldo Cedraz. Processo TCU 000.390/2010-0. Ata 33/2010. Sessão de 08/09/2010. Disponível em: http://portal2.tcu.gov.br/portal/page/portal/TCU/comunidades/tecnologia_informacao/pesquisas_governanca/D500E3BC0A19993DE040010A8900136B. Acesso em 12 nov. 2013.
6. BRASIL. Tribunal de Contas da União. **Acórdão n.º 2.585/2012**. Plenário. Relator: Ministro Walton Alencar Rodrigues. Processo TCU 007.887/2012-4. Ata 38/2012. Sessão de 26/09/2012. Disponível em: http://portal2.tcu.gov.br/portal/page/portal/TCU/comunidades/tecnologia_informacao/pesquisas_governanca/D500BE942EEF7793E040010A89001367. Acesso em 12 nov. 2013.
7. BUGARIN, P. S. **O princípio constitucional da economicidade na jurisprudência do Tribunal de Contas da União**. Belo Horizonte: Fórum, 2004.
8. CHIAVENATO, I. **Administração Geral e Pública**. Rio de Janeiro: Elsevier, 2006.
9. FERNANDES, A. A.; ABREU, V. F. de. **Implantando a Governança de TI: da Estratégia à Gestão dos Processos e Serviços**. 3ª edição. Rio de Janeiro: Brasport, 2012.
10. IT GOVERNANCE INSTITUTE. **CobiT 4.1**. USA, 2012.
11. ITSMF. **An Introductory Overview of ITIL® v3**. United Kingdom, 2007.

12. MAGALHÃES, R. S. P. **Governança em Organizações Públicas - Desafios para entender os fatores críticos de sucesso: O caso do Tribunal de Contras da União**. 2011. 74 p. Dissertação (Mestrado em Administração Pública) - Escola Brasileira de Administração Pública e de Empresas, Fundação Getúlio Vargas, Rio de Janeiro.
13. PROJECT MANAGEMENT INSTITUTE. **PMBOK®: Um Guia do Conjunto de Conhecimentos em Gerenciamento de Projetos**, 4ª edição. São Paulo: Saraiva, 2012.
14. WEILL, P; ROSS, J. W. **Governança de TI: Tecnologia da Informação**. São Paulo: M Books, 2004.